

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Inventory of existing and missing competencies for depicted roles.                                                                                           | GAP      |         | Value of Competency |               |               |                               | RRT Competencies |            |           |                  |              | Courses       |               |               |               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|---------------------|---------------|---------------|-------------------------------|------------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Competencies                                                                                                                                                 | Achieved | Desired | Not Applicable (1)  | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder  | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
| Tier 1: Personal Effectiveness Competencies                                                                                                                  |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| <u>Interpersonal Skills: Displaying the skills to work effectively with others from diverse backgrounds.</u>                                                 |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Demonstrating sensitivity/empathy                                                                                                                            |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Show sincere interest in others and their concerns                                                                                                           |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Demonstrate sensitivity to the needs and feelings of others                                                                                                  |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Look for ways to help people and deliver assistance                                                                                                          |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Demonstrating insight into behavior                                                                                                                          |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Recognize and accurately interpret the verbal and nonverbal behavior of others                                                                               |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Recognize when relationships with others are strained                                                                                                        |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Show understanding of others' behaviors and motives by demonstrating appropriate responses                                                                   |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Demonstrate flexibility for change based on the ideas and actions of others                                                                                  |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Maintaining open relationships                                                                                                                               |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Maintain open lines of communication with others                                                                                                             |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Encourage others to share problems and successes                                                                                                             |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Establish a high degree of trust and credibility with others                                                                                                 |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Respecting diversity                                                                                                                                         |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Interact respectfully and cooperatively with others who are of a different race, culture, or age, or have different abilities, gender, or sexual orientation |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Demonstrate sensitivity, flexibility, and open-mindedness when dealing with different values, beliefs, perspectives, customs, or opinions                    |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Value an environment that supports and accommodates a diversity of people and ideas                                                                          |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| <u>Integrity: Displaying strong moral principles and work ethic.</u>                                                                                         |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Behaving ethically                                                                                                                                           |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Abide by a strict code of ethics and behavior                                                                                                                |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Choose an ethical course of action and do the right thing, even in the face of opposition                                                                    |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |
| Encourage others to behave ethically                                                                                                                         |          |         |                     |               |               |                               |                  |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                               | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Use company time and property responsibly                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Perform work-related duties according to laws, regulations, contract provisions, and company policies                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand that behaving ethically may go beyond what the law requires                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Acting fairly</b>                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Treat others with honesty, fairness, and respect                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Make decisions that are objective and reflect the just treatment of others                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Taking responsibility</b>                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Take responsibility for accomplishing work goals within accepted timeframes                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Accept responsibility for one's decisions and actions and for those of one's group, team, or department                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Learn from mistakes                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Professionalism: Maintaining a professional presence.</u></b>                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Demonstrating self-control</b>                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Maintain composure and keep emotions in check                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Deal calmly and effectively with stressful or difficult situations                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Accept criticism tactfully and attempt to learn from it                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Maintaining a professional appearance</b>                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Maintain a professional demeanor                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Dress appropriately for occupational and worksite requirements                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Maintain appropriate personal hygiene                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Social responsibility</b>                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Refrain from lifestyle choices which negatively impact the workplace and individual performance                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Remain free from substance abuse                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Maintaining a positive attitude</b>                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Project a professional image of oneself and the organization                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate a positive attitude towards work                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Take pride in one's work and the work of the organization                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Initiative: Demonstrating a commitment to effective job performance by taking action on one's own and following through to get the job done.</u></b> |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-----------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| <b>Persisting</b>                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Pursue work with drive and a strong accomplishment orientation                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Persist and expend extra effort to accomplish tasks even when conditions are difficult or deadlines are tight               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Persist at a task or problem despite obstacles or setbacks                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Taking initiative</b>                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Go beyond the routine demands of the job                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Take initiative in seeking out new work challenges and increasing the variety and scope of one's job                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Seek opportunities to influence events and originate action                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Assist others who have less experience or have heavy workloads                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Provide suggestions for innovative approaches to improve processes or tasks                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Setting challenging goals</b>                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Establish and maintain personally challenging but realistic work goals                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Exert effort toward task mastery                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Bring issues to closure by pushing forward until a resolution is achieved                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Working independently</b>                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Develop one's own ways of working effectively and efficiently                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Perform effectively, even with minimal direction, support, or approval                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Take responsibility for completing one's own work assignments                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Achievement motivation</b>                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Strive to exceed standards and expectations                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Exhibit confidence in capabilities and an expectation to succeed in future activities                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Adaptability and Flexibility: Displaying the capability to adapt to new, different, or changing requirements.</u></b> |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Entertaining new ideas</b>                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Remain open to considering new ways of doing things                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Actively seek out and carefully consider the merits of new approaches to work                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Embrace new approaches when appropriate and discard approaches that are no longer working                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Dealing with change</b>                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                              | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Take proper and effective action when necessary without having all the necessary facts in hand                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Easily adapt plans, goals, actions or priorities in response to unpredictable or unexpected events, pressures, situations and job demands |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Easily shift gears and change direction when working on multiple projects or issues                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Dependability and Reliability: Displaying responsible behaviors at work.</u></b>                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Fulfilling obligations</b>                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Behave consistently and predictably                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Is reliable, responsible, and dependable in fulfilling obligations                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Diligently follow through on commitments and consistently complete assignments by deadlines                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Attendance and punctuality</b>                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Come to work on time and as scheduled                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Arrive on time for meetings or appointments                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Dial in to phone calls and web conferences on time                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Attending to details</b>                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Diligently check work to ensure that all essential details have been considered                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Notice errors or inconsistencies, and take prompt, thorough action to correct them                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Following directions</b>                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Follow written and verbal directions                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Comply with organizational rules, policies, and procedures                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Ask appropriate questions to clarify any instructional ambiguities                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Lifelong Learning: Demonstrating a commitment to self-development and improvement of knowledge and skills.</u></b>                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Demonstrating an interest in learning</b>                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate an interest in personal and professional lifelong learning and development                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Seek feedback from multiple sources about how to improve and develop                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Modify behavior based on feedback or self-analysis of past mistakes                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Learn and accept help from supervisors and co-workers                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Participating in training</b>                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                                            | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Identify when it is necessary to acquire new knowledge and skills                                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Take steps to develop and maintain knowledge, skills, and expertise necessary to perform one's role successfully by participating in relevant training and professional development programs                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Actively pursue opportunities to broaden knowledge and skills through seminars, conferences, professional groups, reading publications, job shadowing, and/or continuing education                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Anticipating changes in work</b>                                                                                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Anticipate changes in work demands and search for and participate in assignments or training that address these changing demands                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Treat unexpected circumstances as opportunities to learn                                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Identifying career interests</b>                                                                                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Take charge of personal career development by identifying occupational interests, strengths, options, and opportunities                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Make insightful career planning decisions based on integration and consideration of others' feedback                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Integrating and applying learning</b>                                                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Integrate newly-learned knowledge and skills with existing knowledge and skills                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use newly-learned knowledge and skills to complete tasks, particularly in new or unfamiliar situations                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Tier 2: Academic Competencies</b>                                                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Reading: Understanding written sentences, paragraphs, and figures in work-related documents (with accommodation if necessary).</u></b>                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Comprehension</b>                                                                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Locate and understand written information in prose and in documents such as manuals, reports, memos, letters, forms, graphs, charts, tables, calendars, schedules, signs, notices, applications, contracts, regulations, and directions |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand the purpose of written materials                                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Comprehend meaning and identify main ideas                                                                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Attention to detail</b>                                                                                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Note details and facts                                                                                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Detect inconsistencies                                                                                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify implied meaning and details                                                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify missing information                                                                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                          | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| <b>Information analysis</b>                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Critically evaluate and analyze information in written materials                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Review written information for completeness and relevance                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Distinguish fact from opinion                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify trends                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Synthesize information from multiple written materials                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Information integration</b>                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Integrate what is learned from written materials with prior knowledge                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use what is learned from written material to follow instructions and complete tasks                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Apply what is learned from written material to new situations                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Writing: Using standard (business) English to compile information and prepare written documents.</u></b>                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Organization and development</b>                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Create documents such as letters, directions, manuals, reports, graphs, and flow charts                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Communicate thoughts, ideas, information, messages, and other written information, which may contain technical material, in a logical, organized, and coherent manner |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Present well developed ideas supported by information and examples                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Proofread finished documents for errors                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Tailor content to appropriate audience and purpose                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Distribute written material appropriately for intended audience and purpose                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Mechanics</b>                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use standard syntax and sentence structure                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use correct spelling, punctuation, and capitalization                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use correct grammar (e.g., correct tense, subject-verb agreement, no missing words)                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Write legibly                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Tone</b>                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use language appropriate for the target audience                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use a tone and word choice appropriate for the industry and organization (e.g., writing is professional and courteous)                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                     | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|--------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Show insight, perception, and depth in writing                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Mathematics: Using principles of mathematics to express ideas and solve problems.</u></b>                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Quantification</b>                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Read and write numbers                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Count and place numbers in sequence                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Recognize whether one number is larger than another                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand relationships between numbers                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify and understand patterns                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Computation</b>                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Add, subtract, multiply, and divide with whole numbers, fractions, decimals, and percents                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Calculate averages, ratios, proportions, and rates                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Convert decimals to fractions and fractions to decimals                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Convert fractions to percents and percents to fractions                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Convert decimals to percents and percents to decimals                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Measurement and estimation</b>                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Take measurements of time, temperature, distances, length, width, height, perimeter, area, volume, weight, velocity, and speed                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use and report measurements correctly                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Correctly convert from one measurement to another (e.g., from English to metric or International System of Units [SI], or Fahrenheit to Celsius) |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Application</b>                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Translate practical problems into useful mathematical expressions                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use appropriate mathematical formulas and techniques to solve problems                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Science and Technology: Using scientific rules and methods to express ideas and solve problems</u></b>                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Comprehension</b>                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand basic scientific principles and use appropriate technology                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand the scientific method (i.e., identify problem, collect information, form opinion and draw conclusions)                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand overall intent and proper procedures for set-up and operation of equipment                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                              | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| <b>Application</b>                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Apply basic scientific principles and technology to complete tasks                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Scientific Investigation</b>                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Formulate scientifically investigable questions, construct investigations, collect and evaluate data, and develop scientific recommendations based on findings            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Evaluate scientific constructs including: conclusions, conflicting data, controls, data, inferences, limitations, questions, sources of errors, and variables.            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Communication: Listening, speaking, and signaling so others can understand (with accommodation if necessary).</u></b>                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Listening or attending to information</b>                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Receive, attend to, understand, interpret, and respond to verbal messages and other cues                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Recognize important information in verbal messages                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Comprehend complex instructions                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify feelings and concerns within verbal messages                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Consider others' viewpoints and alter opinion when it is appropriate to do so                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Apply active listening skills using reflection, restatement, questioning, and clarification                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Effectively answer questions of others or communicate an inability to do so and suggest other sources of answers                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Communicating (verbally, either directly, through assistive technology, or other accommodation)</b>                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Express relevant information appropriately to individuals or groups taking into account the audience and the nature of the information (e.g., technical or controversial) |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Convey information clearly, correctly, and succinctly                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use common English conventions including proper grammar, tone and pace                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Track audience responses and react appropriately to those responses                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Effectively use eye contact and non-verbal expression                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Persuasion/influence</b>                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Influence others                                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Persuasively present thoughts and ideas                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Gain commitment and ensure support for proposed ideas                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Observing carefully</b>                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                                                                                                                                                                                               | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Attend to nonverbal cues and respond appropriately                                                                                                                                                                                                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Attend to visual sources of information (e.g., video)                                                                                                                                                                                                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Ascertain relevant visual information and use appropriately                                                                                                                                                                                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Critical and Analytic Thinking: Using logical thought processes to analyze information and draw conclusions.</u></b>                                                                                                                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Reasoning</b>                                                                                                                                                                                                                                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Possess sufficient inductive, and deductive reasoning ability to perform job successfully                                                                                                                                                                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Critically review, analyze, synthesize, compare, and interpret information                                                                                                                                                                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Draw conclusions from relevant and/or missing information                                                                                                                                                                                                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand the principles underlying the relationship among facts and apply this understanding when solving problems                                                                                                                                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use logic and reasoning to identify strengths and weaknesses of alternate solutions or approaches to a problem                                                                                                                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Mental agility</b>                                                                                                                                                                                                                                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify connections between issues                                                                                                                                                                                                                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Quickly understand, orient to, and learn new assignments                                                                                                                                                                                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Fundamental IT User Skills: Using a computer, communication devices, and related applications to input, retrieve, and communicate information.</u></b>                                                                                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>General Computer, Software, Information and Communication Technology Knowledge and Skills</b>                                                                                                                                                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate familiarity with the fundamental capabilities of computers, software, information systems, and communications systems                                                                                                                                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate familiarity with the fundamental principles of accessible technology, including universal design, as they relate to users of computerized content who have disabilities, sensory and/or functional limitations                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand terminology and function of common computer, software, information and communication technology devices, components, and concepts                                                                                                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand common terminology related to the use of technology by people with disabilities and/or sensory and functional limitations, including accessible IT, assistive technology, and universal design                                                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand and efficiently use common computer hardware (e.g., desktops, laptops, tablets, PC components, cabling, wearable computing), software (e.g., operating systems, applications, communication, collaboration and productivity software), and communication devices (e.g., telephony, wireless devices, network and wireless systems) to perform tasks and communicate effectively |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware within data centers or the "cloud"                                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                           | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Understand network hardware devices and functions                                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Be able to connect common User devices to networks and secure them appropriately                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand and be able to use with appropriate etiquette common communications media, including wired and wireless telephones, wearable computing, audio conferences, videoconferences, and online collaboration tools |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use a computer to search for online information and interact with websites and web applications (enterprise solutions, online stores, blogs, social networks, wikis)                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand how to critically evaluate online information and be aware of relevant intellectual property, patent, copyright, and data protection issues                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand the characteristics of physical and virtual data storage media                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to interpret and incorporate data from multiple tool sources                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Digital Literacy</b>                                                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to create authentic meaningful written and artwork by reproducing and manipulating preexisting digital text, visuals, and audio pieces                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to construct knowledge by a nonlinear navigation through knowledge domains, such as in the Internet and other hypermedia environments                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to critically evaluate the textual characteristics of digital media alongside their social, economic and cultural implications                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Visualize graphic representation of concepts or data                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Common IT Applications Use</b>                                                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use word processing applications to compose, organize, and edit simple documents and other business communications and produce accurate outputs to print or share electronically                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use standard formulas and functions, format and modify content, and demonstrate competence in creating and formatting spreadsheets, graphs, or charts                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use spatial software to locate places and interpret spatial data                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use and manage electronic mail to communicate with appropriate etiquette                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use Internet applications to search for information                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use presentation software to effectively share information and ideas                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use spreadsheet, database, and presentation software both independently and in an integrated fashion                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use audio and video recording equipment and software to produce digital audio and video records and communications                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use file storage applications to store, retrieve, and sort documents                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                                                | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Understand social media and their appropriate workplace uses and non-workplaces uses, and the impact that various social media activities can have upon one's personal and professional life                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Double check work carefully and identify/correct typographical, grammatical, and other errors                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Information and Research Literacy</b>                                                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Define: Be able to define a problem that needs information in order to be solved                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Access: Search, find, and retrieve appropriate information relative to the task                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Manage: Apply an organizational or classification system to organize retrieved information                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Evaluate: Be able to judge the quality, relevance, usefulness, efficiency, and adequacy of information and information sources for the defined purpose (including authority, bias, and timeliness of information)                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Integrate: Interpret and represent data and information gathered, using quality management tools to organize, compare, contrast, summarize, and synthesize information from multiple sources                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Create: Adapt, apply, design, or author information resulting from the research that describes the research and its analysis and findings, facilitates decision-making, and develops conclusions and recommendations                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Communicate: Communicate that research and its findings effectively and efficiently in person and through written, visual, and digital media in a way that is appropriate for the intended audience                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Hardware</b>                                                                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate competence with the following technology:                                                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Central processing unit (CPU)                                                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Memory - random-access memory (RAM) and read-only memory (ROM)                                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Storage media, (e.g., internal hard disk, external hard disk, network drive, CD, DVD, USB, flash drive, memory card)                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Input/output ports, (e.g., USB, serial, parallel, network port, FireWire)                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Input devices, (e.g., mouse; keyboard; trackball; scanner; touchpad; stylus; joystick; web camera; digital camera; microphone; voice recognition; remote control; gesture/motion; haptics; and head, mouth, and eye operated controllers) |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Output devices, (e.g., screens/monitors, printers, speakers, headphones, wearable computing)                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Assistive technology devices, (e.g., voice recognition software, screen reader, screen magnifier, on-screen keyboard, closed captioning, gesture/motion, haptics, text-to-speech)                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Database Management Systems</b>                                                                                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines)                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand database management systems, query languages, table relationships, and views                                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                          | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Demonstrate skill in generating queries and reports                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Operating Systems</b>                                                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand server and client operating systems                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand systems administration concepts                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip)                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand how to troubleshoot basic systems and identify operating systems-related issues                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate skill in identifying, modifying, and manipulating applicable system components (Windows and/or Unix/Linux) (e.g., passwords, user accounts, files)                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Systems Integration</b>                                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand how system components are installed, integrated, and optimized                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand technology integration processes                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand web services, Service Oriented Architecture (SOA) and Application programming Interfaces (APIs)                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Technology Awareness</b>                                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand new and emerging IT and information security technologies                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate skill in applying and incorporating information technologies into proposed solutions                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand products and nomenclature of major vendors (e.g., security suites: Trend Micro, Symantec, McAfee, Outpost, Panda, Kaspersky, etc.) and how differences affect exploitation/vulnerabilities |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand the capabilities and functionality associated with various content creation technologies (e.g., wikis, social networking, blogs)                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint, wikis, blogs, web collaborations)                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand industry indicators useful for identifying technology trends                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Tier 3: Workplace Competencies</b>                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Teamwork: Working cooperatively with others to complete work assignments.</u></b>                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Acknowledging team membership and role</b>                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Accept membership in and commit to the goals of the team                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Show loyalty to the team                                                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Serve as a leader or a follower, depending on what is needed to achieve the team's goals and objectives                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Guide others in learning new skills                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                      | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|---------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Encourage others to express their ideas and opinions                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify and draw upon team members' strengths and weaknesses to achieve results                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Learn from other team members                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Establishing productive relationships</b>                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Develop constructive and cooperative working relationships with others                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Exhibit tact and diplomacy and strive to build consensus                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Deliver constructive criticism and voice objections to others' ideas and opinions in a supportive, non-accusatory manner                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Respond appropriately to positive and negative feedback                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Identifying with the team and its goals</b>                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Work as part of a team, contributing to the group's effort to achieve goals                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify the goals, norms, values, and customs of the team                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Choose behaviors and actions that best support the team and accomplishment of work tasks                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use a group approach to identify problems and develop solutions based on group consensus                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Effectively communicate with all members of the group or team to achieve team goals and objectives                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Resolving conflicts</b>                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Bring others together to reconcile differences                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Handle conflicts maturely by exercising "give and take" to achieve positive results for all parties                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Reach formal or informal agreements that promote mutual goals and interests, and obtain commitment to those agreements from individuals or groups |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Planning and Organizing: Planning and prioritizing work to manage time effectively and accomplish assigned tasks.</b>                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Planning</b>                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Approach work in a methodical manner                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Plan and schedule tasks so that work is completed on time                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Keep track of details to ensure work is performed accurately and completely                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Anticipate obstacles to project completion and develop contingency plans to address them                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Find new ways of organizing work areas or planning work to accomplish work more efficiently                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Prioritizing</b>                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                  | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Prioritize multiple competing tasks                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Perform tasks quickly, correctly, and efficiently according to their urgency                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Managing projects</b>                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Estimate personnel and other resources needed for project completion (e.g., financial material or equipment)                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Manage activities to meet plans, allocating time and resources effectively                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Keep track of and documents plans, assignments, changes, and deliverable                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Plan for dependencies of one task on another                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Coordinate efforts with all affected parties, keeping them informed of progress and all relevant changes to project timelines |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Take necessary corrective action when projects go off-track                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Creative Thinking: Generating innovative and creative solutions.</u></b>                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Employing unique analyses</b>                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use original analyses and generate new, innovative ideas in complex areas                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Develop innovative methods of obtaining or using resources when insufficient resources are available                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Generating innovative solutions</b>                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Integrate seemingly unrelated information to develop creative processes or solutions                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Reframe problems in a different light to find fresh approaches                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Entertain wide-ranging possibilities and perspectives to develop new solutions                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Find new ways to add value to the efforts of a team and organization                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Seeing the big picture</b>                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand the pieces of a system as a whole and appreciate the consequences of actions to other parts of the system          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Monitor patterns and trends to see a bigger picture                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Modify or designs systems to improve performance                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Problem Solving and Decision-Making: Generating, evaluating, and implementing solutions.</u></b>                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Identifying the Problem</b>                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Anticipate or recognize the existence of a problem                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify the true nature of the problem and define critical issues                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                               | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Evaluate the importance and criticality of the problem                                                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use all available reference systems to locate and obtain information relevant to understanding the problem                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Recall previously learned information that is relevant to the problem                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Locating, gathering, and organizing relevant information</b>                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Effectively use both internal resources (e.g., internal computer networks, company filing systems) and external resources (e.g., internet search engines) to locate and gather information relevant to solving the problem |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Examine information obtained for relevance and completeness                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Recognize important gaps in existing information and take steps to eliminate those gaps                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Organize/reorganize information as appropriate to gain a better understanding of the problem                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Generating alternatives</b>                                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Integrate previously learned and externally obtained information to generate a variety of high-quality alternative approaches to the problem                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Skilfully use logic and analysis to identify the strengths and weaknesses, the costs and benefits, and the short- and long-term consequences of different solutions or approaches                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Choosing a Solution</b>                                                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Decisively choose the best solution after evaluating the relative merits of each possible option                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Make difficult decisions even in highly ambiguous or ill-defined situations                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Implementing the solution</b>                                                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Commit to a solution in a timely manner                                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Develop a realistic approach for implementing the chosen solution                                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Document the problem and corrective actions taken and their outcomes and communicate these to the appropriate parties                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Observe and evaluate the outcomes of implementing the solution to assess the need for alternative approaches and to identify lessons learned                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Working with Tools and Technology: Selecting, using, and maintaining tools and technology to facilitate work activity (with accommodation when necessary).</u></b>                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Using tools</b>                                                                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Operate tools, technology, and equipment in accordance with established operating procedures and safety standards                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate appropriate use of tools and technology to complete work functions                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Selecting tools</b>                                                                                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                      | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Select and apply appropriate tools or technological solutions to the problem at hand                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Keeping current</b>                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate an interest in learning about new and emerging tools and technologies                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Adapt quickly to changes in process or technology                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Seek out opportunities to improve knowledge of tools and technologies that may assist in streamlining work and improving productivity                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Troubleshooting and maintenance</b>                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Learn how to maintain and troubleshoot tools and technologies                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Perform routine maintenance on tools, technology, and equipment                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Determine causes of errors and take the appropriate corrective action                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Develop alternatives to complete a task if desired tool or technology is not available                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Business Fundamentals: Using information on basic business principles, trends, and economics.</u></b>                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Situational Awareness</b>                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand the mission, structure, and functions of the organization                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Recognize one's role in the functioning of the organization and understand the potential impact one's own performance can have on the success of the organization |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Grasp the potential impact of the organizations well-being on employees                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Business Ethics</b>                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate respect for coworkers, colleagues, and customers                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Act in the best interest of the company, the community, and the environment                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Comply with applicable laws and rules governing work and report loss, waste, or theft of company property to appropriate personnel                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Business Practices</b>                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand fundamental and relevant business customer and supplier relationships                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use product improvement techniques                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Comply with the norms of conventional business etiquette                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Protect intellectual property and proprietary information                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate understanding of the importance of adding value to the enterprise                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Global Awareness</b>                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                         | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Understand how IT supports globalization                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand the impact of globalization on the business model                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Interpret and adhere to global standards and standardization                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Market knowledge</b>                                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand market trends in the industry and company's position in the market                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Know who the company's primary competitors are and stay current on organizational strategies to maintain competitiveness                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Uphold the organization through building and maintaining customer relations                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Recognize major challenges faced by the organization and industry and key strategies to address challenges                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Tier 4: Cyber Security Technical Competencies</b>                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <u><b>Cybersecurity Technology: The knowledge, skills, and abilities needed to understand the purpose and function of cybersecurity technology, including tools and systems.</b></u> |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Critical Work Functions:</b>                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Cryptography</b>                                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the core concepts of cryptography and cryptographic key management concepts                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the concept of public key infrastructure (PKI)                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain symmetric key rotation techniques and concepts                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe encryption methodologies                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Information Technology (IT) Architecture</b>                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain IT architectural concepts and frameworks                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain security system design tools, methods, and techniques                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate knowledge of information theory                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate knowledge of communication methods, principles, and concepts                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain parallel and distributed computing concepts                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain remote access technology concepts                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe how different file types can be used for anomalous behavior                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Distinguish between data in use, data in motion (transit), and data at rest                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe the capabilities of different electronic communication systems and methods                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|---------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Understand system life cycle management principles, including software security and usability                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Operational Technology (OT) Architecture</b>                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain typical OT architecture                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Differentiate between IT and OT architectures and the operation of these architectures                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the typical communications network options and communications protocols used in OT architectures, with their relative pros and cons |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify the principal drivers of OT systems, particularly process safety and system availability                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Networks</b>                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain computer networking concepts and protocols, and network security methodologies                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain network design processes, to include understanding of security objectives, operational objectives, and tradeoffs                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain local area network (LAN) and wide area network (WAN) principles and concepts, including bandwidth management                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, v3 [ITIL])     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify the range of existing networks types                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain how traffic flows across the network                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain server administration and systems engineering theories, concepts, and methods                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify host and network access control mechanisms (e.g., access control list)                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Recognize the impact on OT systems of security hardware and software options such as encryption and intrusion detection                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain guidance on separation of OT and IT system networks and components                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe basic system administration, network, and operating system hardening techniques                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Operating Systems</b>                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate familiarity with the security features and functions of common operating systems                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain virtualization technologies and virtual machine development and maintenance                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe how to manage patches to IT and OT operating systems                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Recognize the implications of installed patches to IT and OT systems                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate familiarity with Windows command line                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                      | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Demonstrate familiarity with Unix/Linux operating system structure and internals (e.g., process management, directory structure, installed applications)                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify file system implementations                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate familiarity with Windows/Unix/Android, iOS, and Windows Mobile ports and services                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Security Technology Awareness</b>                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand emerging security issues, risks, and vulnerabilities                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify emerging computer-based technology that has potential for exploitation by adversaries                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate skill in applying and incorporating new and emerging cybersecurity technologies and trends into proposed solutions                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand products and nomenclature of major IT security vendors and how differences affect exploitation/vulnerabilities                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Telecommunications</b>                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain basic concepts, terminology, and operations of a wide range of communications media                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe transmission methods and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe the communications protocols used in OT architectures, with their relative pros and cons                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand Voice over Internet Protocols (VoIPs)                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Web Technologies</b>                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain web services, including service oriented architecture, Representational State Transfer (REST), Simple Object Access Protocol (SOAP), and web service description language |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain web filtering technologies                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Technical Content Areas:</b>                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Cryptography</b>                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Core concepts and methodologies                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Encryption concepts (e.g., symmetric vs. asymmetric, transport encryption, digital signatures)                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Cryptographic tools and products (e.g., WEP, MD5, SHA)                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Public Key Infrastructure (PKI)                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Certificate authorities and digital certificates                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                             | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|----------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| o Recovery agent                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Registration                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Key escrow                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Trust models                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>IT Architecture</b>                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Electronic communication systems and methods             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o E-mail                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Voice over Internet Protocol (VoIP)                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Instant Messenger (IM)                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Web forums                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Direct video broadcasts                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Information theory                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Source coding                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Channel coding                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Algorithm complexity theory                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Data compression                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Communication methods, principles, and concepts, such as |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Encoding                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Signaling                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Multiplexing                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>OT Architecture</b>                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Architecture concepts                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Sensors                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o PLC/RTU                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Fieldbus                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Supervisory Control and Data Acquisition (SCADA)       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o HMI                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                             | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|----------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| o DCS                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Historians                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Networks</b>                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Architecture concepts                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Topology                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Components (e.g., firewalls, routers, switches)                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Network Types, such as                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Local Area Networks (LANs)                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Wide Area Networks (WANs)                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Wireless Fidelity (Wi-Fi)                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Private Branching Exchange (PBX)                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Sensor networks                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Network Protocols, such as                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Transmission Control Protocol and Internet Protocol (TCP/IP)                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Dynamic Host Configuration Protocol (DHCP)                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Domain Name System (DNS)                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o IPv4 and IPv6                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Hardening Techniques                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Hardware-based computer protection components (e.g., hardware firewalls, servers, routers)             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware) |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Operating Systems</b>                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Common Operating Systems (OS)                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Windows                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Unix/Linux                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Mac OS                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Android                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o iOS                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                           | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| o Windows Mobile                                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| File system implementations, such as                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o New Technology File System (NTFS)                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o File Allocation Table (FAT)                                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o File Extension (EXT)                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Telecommunications</b>                                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Concepts                                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Routing algorithms                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Fiber optics systems link budgeting                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Add/drop multiplexers                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Communication media, such as                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Computer and telephone networks                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Satellite                                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Fiber                                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Wireless                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Transmission methods, such as                                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Bluetooth                                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Radio Frequency Identification (RFID)                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Infrared Networking (IR)                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Wireless Fidelity (Wi-Fi)                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Cellular                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Satellite dishes                                                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| OT communication protocols, such as                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o DNP3                                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Modbus                                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o IEC60870                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Information Assurance: The standards, procedures, and applications used to protect the confidentiality, integrity and availability of information(CIA) and information systems.</b> |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                          | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| <b>Critical Work Functions:</b>                                                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Information Assurance</b>                                                                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Apply confidentiality, integrity, and availability principles                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain key concepts in security management (e.g., release management, patch management)                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain how information assurance principles and methods apply to software development                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe Security Assessment and Authorization (SA&A) process                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Data Management</b>                                                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain data classification standards and methodologies based on sensitivity and other risk factors                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the importance of complying with data management policies                                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the need for an organization to understand what its sensitive information is, where it resides, and who needs access to it                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate knowledge of advanced data remediation security features in databases                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to manage data stored within operational technology (OT) systems (e.g., time series data stored in Supervisory Control and Data Acquisition [SCADA] and Historians)                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the need to track the movement of data across network boundaries both electronically and physically                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the need to limit USB and other removable media reading and writing capabilities on organization computers                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Adhere to data administration and data standardization policies and standards                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain data mining and data warehousing principles                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify sources, characteristics, and uses of the organization's data assets                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Common Strategies for Ensuring Information</b>                                                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to produce copies of all data or information used in or generated by the organization                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to backup and store data automatically on a separate hard disk, off-line removable media, or online storage                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to protect sensitive information when disposing of old computers and media                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the need to limit access or use of an organization's computers, including laptops, to unauthorized persons                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                             | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Explain the concept of administrative privileges and administrative user accounts and why it is necessary to restrict them to select individuals within the organization |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain digital rights management                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Identity Management and Authentication</b>                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain key authentication, authorization, and access control principles and methods                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the need for access authentication controls, including the need to disable expired user accounts and regularly change passwords                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Adhere to organizational information technology user security policies                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Adhere to Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Technical Content Areas:</b>                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Information Assurance</b>                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Principles of Information Assurance                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Asset value                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Confidentiality, integrity, and availability (the CIA triad)                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Principal of least privilege                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Access control                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Separation of duties                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Data Management</b>                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Data mining and warehousing principles                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Data integrity                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Data protection (e.g., encryption, masking)                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Data loss prevention techniques and tools                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Privacy impact assessments                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Common Strategies for Ensuring Information</b>                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Data and information to be safeguarded, such as                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Word processing documents                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Electronic spreadsheets                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Databases                                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                            | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|---------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| o Financial files                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Human resources rules                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Accounts receivable and payable                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Data management policies, such as those pertaining to   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Storage media                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Transmission archiving                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Retention requirements                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Data destruction                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Deduplication                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Data loss prevention                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Social network usage                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Information rights usage                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Identity Management and Authentication</b>           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Key principles and concepts                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Identification vs. authentication                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Single factor authentication and authorization        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Multifactor authentication                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Authentication controls, such as                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Biometrics                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Tokens                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Common access card                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Personal identification verification card             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Authentication services (e.g., RADIUS, TACAS, OpenID) |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| User security policies, such as                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Account creation                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Password rules                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Access controls                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                                              | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| <b>Risk Management: The systems, tools, and concepts used to minimize the risk to an organization's cyberspace and prevent a cybersecurity incident.</b>                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Critical Work Functions:</b>                                                                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Business Continuity Planning</b>                                                                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain and justify each step of the Business Continuity Planning process:                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Identify critical business practices (such as complex regional or global supply chain strategies) that may adversely impact the entity's ability to recover following a disaster event                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Clearly define resource requirements for the Business Continuity Plan (BCP) and solicit management support and commitment for required resources                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Present and obtain management/leadership support, approval, and sponsors of BCP                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Work with management and any risk management/enterprise risk management groups within the entity to gain agreement on a clear and standardized risk assessment methodology and to gain understanding of the entity's tolerance for risk |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Design a crisis communications plan that addresses the need for effective and timely communication between the entity and all the stakeholders impacted by an event or involved during the response and recovery efforts                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Provide guidance within the plan to determine frequency of communications needed to each stakeholder before an event, during the event itself, and following an event                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Identify and establish relationships with the internal departments and personnel and external agencies, contractors, and others with responsibility for emergency preparedness and response                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Develop an incident response strategy and plan to limit incident effect and to repair incident damage                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Identify trigger points for key service and support areas to identify, escalate and execute strategies selected to take advantage of key risks                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Develop formal reports and presentations focused on increasing the awareness and potential impact of risks to the organization from a business continuity perspective                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Define organizational titles, roles, lines of authority, succession of authority, and responsibilities for internal and external resources                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Establish an exercise, testing, maintenance and audit program for the BCP to establish confidence in a predictable and repeatable performance of recovery activities throughout the organization                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Coordinate, conduct, and or participate in training, drills, and exercises with first responders to comply with regulations, as needed to establish required capabilities, and or as requested by first responders                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Conduct a debrief meeting immediately following training, drills and exercises and document actions to be taken to improve emergency preparedness and response capabilities                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                                                   | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| o Design framework and define document structure for the plan documentation                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Define and obtain approval for criteria to be used to assess the impact on the entity's operations including but not limited to: customer impact; financial impact; regulatory impact; operational impact; reputational impact; human impact |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand the risks associated with operational technology (OT) systems and be able to identify practical mitigation measures to manage these risks                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
|                                                                                                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Computer Defense</b>                                                                                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify cyber defense mitigation techniques and vulnerability assessment tools, including open source tools, and their capabilities                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate skill in discerning the protection needs (i.e., security controls) of information systems and networks                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe the impact of computer defense techniques and tools on information technology (IT) and OT systems and know when to use such techniques or tools                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify common adversary tactics, techniques, and procedures (TTPs) in assigned area of responsibility                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain application firewall concepts and functions                                                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Adhere to cyber defense policies, procedures and regulations                                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate skill in collecting data from a variety of cyber defense resources                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Contracting and Procurement</b>                                                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe critical IT and OT procurement requirements                                                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate skill in evaluating the trustworthiness of the supplier and/or product                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes)                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Define secure acquisitions                                                                                                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Enterprise/Organization</b>                                                                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain organizational process improvement concepts and process maturity models                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Recognize the nature and function of the relevant information structure                                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify enterprise/organization security models                                                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify the organization's Information Classification Program and procedures for level information loss                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                                  | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Recognize the specialized system requirements of OT systems                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the organization's core business/mission processes, stakeholders, and users                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate an understanding of the services provided by the enterprise or organization and the elements of the system that support the delivery of these services                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe the Enterprise Network Defense provider reporting structure and processes within the organization                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the need for common metrics that measure the effectiveness of security measures with the organization                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the need for continuous diagnostics and mitigation to test and validate the effectiveness of current security measures                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the need for automated defenses                                                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify local specialized system requirements (e.g., critical infrastructure systems that may not use standard IT for safety, performance, and reliability)                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Risk and Vulnerability Analysis</b>                                                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate knowledge of system and application threats and vulnerabilities                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to identify threats/risks and vulnerabilities taking into account the frequency, probability, speed of development, severity and reputational impact to achieve a holistic view of risk across the entity |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to classify risks according to relevant criteria including, but not limited to:                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Risks under the entity's control                                                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Risks beyond the entity's control                                                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Risks with prior warnings (such as tornadoes and hurricanes)                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Risks with no prior warnings (such as earthquakes)                                                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to identify the organization's risk exposures from both internal and external sources                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the use of network analysis tools to identify software communications vulnerabilities                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the proper use of penetration testing and vulnerability scanning for vulnerability assessments                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the impact of penetration testing and vulnerability scanning on OT systems and know when to use such techniques                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Risk Management Strategies</b>                                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the rationale of and adhere to IT and OT supply chain security/risk management policies, requirements, and procedures                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                                                                                        | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Explain the need for antivirus and antispyware software on all computers used in an organization's operations and the need for continuous auto- or manual-update of this software                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the need to track/control/prevent/correct installation and execution of software on computers based on an asset inventory of approved software                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the need to track/control/prevent/correct network access by devices (computers, network components, printers, BYODs [Bring Your Own Devices], anything with IP addresses) based on an asset inventory of which devices are allowed to connect to the organization's network |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the need for formal configuration management and change control processes                                                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain need for dispersing responsibility and access to data and systems, including financial, personnel, inventory, and manufacturing, over multiple individuals (e.g., one employee should not be allowed to both initiate and approve financial transactions)                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the importance of training an organization's workers to use sensitive business information properly and to protect the organization's and its stakeholders' information                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe and practice safe internet behavior                                                                                                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the risks associated with social media and the countermeasures available to address them                                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the impact and proper use of environmental controls                                                                                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the need for security audit logging and analysis                                                                                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Software Lifecycle</b>                                                                                                                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe the type and frequency of routine maintenance needed to keep equipment functioning properly                                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to install computer upgrades                                                                                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the operations and processes for diagnosing common or recurring system problems                                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to identify and anticipate server performance, availability, capacity, or configuration problems                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Technical Content Areas:</b>                                                                                                                                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Enterprise/Organization Awareness</b>                                                                                                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Process improvement concepts and process maturity models, such as                                                                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Capability Maturity Model Integration (CMMI) for Development                                                                                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o CMMI for Services                                                                                                                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o CMMI for Acquisitions                                                                                                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Security models, such as                                                                                                                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Bell-LaPadula model                                                                                                                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                          | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|---------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| o Biba integrity model                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Clark-Wilson model                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Computer Defense</b>                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Computer defense techniques and tools, such as                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Manual bypassing of electronic controls                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Monitoring system logs                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Physical security (e.g., locks, video surveillance, fencing)                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Hardening (e.g., disabling unnecessary services, protecting management interfaces and applications, disabling unnecessary accounts) |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Port security                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Security postures                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Reporting                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Detection controls vs. prevention controls                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Application firewall concepts and functions                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Single point of authentication/audit/policy enforcement                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Message scanning for malicious content                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Data anonymization for PCI and PII compliance                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Data loss protection                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Risk and Vulnerability Analysis</b>                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| System and application security threats and vulnerabilities, such as                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Buffer overflow                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Mobile code                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Cross-site scripting                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Procedural language/structures query language (PL/SQL) and injections                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Race conditions                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Covert channel                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Replay                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Return-oriented attacks                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                              | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|---------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| o Malicious code                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Internal and external sources of risk:                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Natural                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Technological                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Man-made (e.g., distributed denial-of-service attack (DDoS), social engineering, wireless attacks, application attacks) |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Accidental versus intentional                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Controllable exposures/risks versus those beyond the entity's control                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Events with prior warnings versus those with no prior warnings                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Risk impacts:                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Facility                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Security (both physical and logical)                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Reputational                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Legal                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Customer                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Procedural                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o IT (including operational infrastructure)                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o People                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Supply Chain (including transportation and outsourcing)                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Compliance                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Availability of personnel                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Network Communications technology                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Risk Management Strategies</b>                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Risk management training topics                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Information security policies, including the use of computers, networks and Internet connections                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Limitations on personal use of telephones, printers, and other business resources                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Differences between OT and IT systems                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Restrictions on accessing OT systems at home or outside the secure work areas of the business                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                    | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| o Restrictions on processing business data at home                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Safe internet behavior                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Open only email that is expected and from a sender that is trusted                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Examine carefully web links in email, instant messages, social media, and other communications                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Do not access email or internet on OT system computers                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Do not install unauthorized software on OT system computers                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Close popup windows that request a response                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Conduct online business, commerce, and banking using a secure browser connection                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Visit only web sites with trusted reputations                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Download software only from trusted web sites                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Risks associated with social media                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Data leakage                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Inappropriate posts                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Posts that violate laws or regulations                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Social engineering                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Spreading of false information                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Incident Detection: The knowledge, skills, and abilities needed to identify threats or incidents.</u></b>                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Critical Work Functions:</b>                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Incident Detection</b>                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe what constitutes a network attack and the relationship to both threats and vulnerabilities                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the concepts of packet analysis and intrusion detection                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to differentiate between attacks and normal user activity on a network                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify intrusion detection methodologies and techniques for detecting host and network based intrusions via intrusion detection technologies. |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate skill in identifying capturing, containing, and reporting malware                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate familiarity with Intrusion Detection System (IDS) tools and applications                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the need to analyze an entire network instead of a single device                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify system diagnostic tools and fault identification techniques                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                               | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Identify server diagnostic tools and fault identification techniques                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the concept of zero-day attacks                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe general attack stages                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify virtual machine aware malware, debugger aware malware, and packing                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain malware analysis concepts and methodology                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify malware analysis tools (e.g., Oily Debug, Ida Pro)                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe network analysis methods                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Incident Classification</b>                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe different classes of attacks                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to identify the following characteristics of an incident:                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Origin or location (internal or external)                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Size or magnitude                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Area of impact                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate ability to categorize events (using the organization's standard category definitions) and assign events for further analysis, response, or disposition/closure |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Report the pertinent information to the appropriate individual, group, or process                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Determine the risk, threat level, or business impact of a confirmed incident                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Casualties                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Property damage                                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Operational interruption or disruption                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Environmental contamination                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the importance of collecting incident data and intrusion artifacts (e.g., malware, logs) (to enable mitigation of incidents)                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Determine the risk of continuing operations                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Technical Content Areas</b>                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Incident Detection</b>                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Intrusion detection tools                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Host Based Intrusion Detection Systems (HIDS)                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                     | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| o Network Based Intrusion Detection Systems (NIDS)                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Wireless Intrusion Detection Systems (WIDS)                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Network monitoring resources, such as                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o System logs                                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o History logs                                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o General logs                                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Traffic analysis                                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Network sniffer                                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Attack stages                                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Footprinting and scanning                                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Enumeration                                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Gaining access                                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Escalation of privileges                                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Maintaining access                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Network exploitation                                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Covering tracks                                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Incident Classification</b>                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Attack classes                                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Passive                                                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Active                                                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Insider                                                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Close-in                                                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Distribution                                                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Incident Response and Remediation: The knowledge, skills, and abilities needed to respond to and remediate an incident, as well as restore functionality to the system or infrastructure.</b> |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Critical Work Functions:</b>                                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Business Continuity Plan Implementation</b>                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe enterprise incident response program, roles, and responsibilities, including first responders                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                                        | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Explain and justify each step that occurs during Business Continuity Planning implementation:                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Identify the available continuity and recovery strategies for the entity's operations that will meet the recovery time objective and recovery point objectives identified during the Business Continuity Planning process         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Assess viability of alternative strategies against the results of business impact analysis/recovery time objectives                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Compare solutions                                                                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Advantages                                                                                                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Disadvantages                                                                                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Costs (startup, maintenance & execution)                                                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Mitigation capability and control options                                                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Ability to meet defined RTO and RPO                                                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Estimate the cost of implementing and maintaining recovery for the identified recovery strategies                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Validate that the recovery strategy being implemented is in line with the amount of business at risk                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Identify applicable emergency preparedness and response regulations                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Cooperate with other internal groups (e.g., information technology [IT], operational technology [OT], management, compliance, legal, human resources, etc.) and external agencies according to applicable policies and procedures |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Criminal Law</b>                                                                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify national and international laws, regulations, policies, and ethics as they relate to cybersecurity                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify applicable laws and/or administrative/criminal legal guidelines and procedures relevant to work performed                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain legal rules of electronic evidence and court procedure (e.g., admissibility), such as the Federal Rules of Evidence                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Recognize legal trends that will impact cyber activities                                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Recognize the impact of technology trend data on laws, regulations, and/or policies                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Forensics</b>                                                                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the concepts of data backup, types of backups, and recovery concepts and tools                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe types of digital forensics data and how to recognize them                                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain deployable forensics                                                                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                   | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Recognize anti-forensics tactics, techniques, and procedures                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain concepts and practices of processing digital forensic data                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Identify which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe investigative implications of hardware, operating systems, and network technologies                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the importance of collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data. |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain processes for seizing and preserving digital evidence (e.g., chain of custody)                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Post Incident Activities and Analysis</b>                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Track and document incidents from initial detection through final resolution in support of future analytical efforts and situational awareness                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Assign and label data / information according to the appropriate class or category of sensitivity                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Make appropriate changes to system security to ensure that vulnerabilities leading to incident have been addressed (e.g., change passwords)                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Explain the importance of validating system security prior to resumption of core activities and functions                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Technical Content Areas:</b>                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Criminal Law</b>                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Applicable laws                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Electronic Communications Privacy Act                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Electronic Identification and Trust Services for Electronic Transactions Act                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Code of Criminal Procedure                                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Prosecutor's Office Act                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Procedures for the recording of court sessions and the preparation of a digital protocol                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Search and seizure laws                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Civil liberties and privacy laws                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Electronic Communications Act                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Presidential Directives                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Executive branch guidelines                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o State Secrets and Classified Information of Foreign States Act                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                             | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|----------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| o Organisations Act                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Crisis Communication</b>                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Notification systems                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Email and group distribution lists                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Conference call                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Intranet                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Press conference                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Event information line                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Media sources                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Print                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Radio                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o TV                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Internet                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Social media sites (e.g., Facebook, Twitter, LinkedIn) |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Forensics</b>                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Types of backups                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Full                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Incremental                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Forensic evidence formats, such as                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Hard drives                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Floppy diskettes                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Compact disc (CDs)                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Personal digital assistants (PDAs)                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Mobile phones                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Global positioning satellite devices (GPSs)            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o All tape formats                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Digital forensics data, such as                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                           | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| o Log files                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Registry files                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Configuration files                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Basic forensic procedures                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Order of volatility                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Capture system image                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Network traffic and logs                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Capture video                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Record time offset                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Take hashes                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Screenshots                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Witnesses                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Track man hours and expense                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Post Incident Activities and Analysis</b>                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Types of incident information to be documented                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Strategic, including succession planning                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Tactical                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Operational                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Emergency response                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Incident control and damage assessment                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Continuity and recovery                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| o Return-to-normal operations                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Tier 5: Digital Forensics Field Knowledge Competencies</b>          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Organize and Conduct interviews (recruitment interviews).              |          |         |                    |               |               |                               | 1               | 1          | 1         | 1                | 2            |               |               |               |               |
| Develop a plan to investigate incident utilizing every possible means. |          |         |                    |               |               |                               | 1               | 2          | 2         | 3                | 3            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                 | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Establish useful contacts, (e.g., the incident response team, legal department, law enforcement agencies, vendors, public relations professionals) for better cooperation. ) |          |         |                    |               |               |                               | 1               | 2          | 2         | 3                | 3            |               |               |               |               |
| Examine and analyze recovered data.                                                                                                                                          |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 1            |               |               |               |               |
| Compose cyber attacks analyses.                                                                                                                                              |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Identify and determine whether a security incident is indicative of a violation of law that requires specific legal action.                                                  |          |         |                    |               |               |                               | 3               | 2          | 3         | 3                | 3            |               |               |               |               |
| Identify data or intelligence of evidentiary value to support investigations.                                                                                                |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 3            |               |               |               |               |
| Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.                                                                   |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |
| Identify and distinguish elements of e-evidence.                                                                                                                             |          |         |                    |               |               |                               | 3               | 2          | 2         | 2                | 3            |               |               |               |               |
| Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations.  |          |         |                    |               |               |                               | 3               | 3          | 2         | 2                | 3            |               |               |               |               |
| Identify documentation needed for crime scene processing.                                                                                                                    |          |         |                    |               |               |                               | 3               | 2          | 2         | 2                | 3            |               |               |               |               |
| Prepare and process crime scenes.                                                                                                                                            |          |         |                    |               |               |                               | 3               | 2          | 2         | 2                | 3            |               |               |               |               |
| Collect and secure the electronic device or information source.                                                                                                              |          |         |                    |               |               |                               | 3               | 2          | 2         | 2                | 3            |               |               |               |               |
| Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.                                                     |          |         |                    |               |               |                               | 3               | 2          | 2         | 1                | 3            |               |               |               |               |
| Construct and manage deployable digital forensics toolkit (e.g., specialized software/hardware) to support Incident Response Team mission.                                   |          |         |                    |               |               |                               | 3               | 3          | 2         | 1                | 3            |               |               |               |               |
| Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks.                                                                        |          |         |                    |               |               |                               | 2               | 2          | 2         | 2                | 3            |               |               |               |               |
| Arrange criminal investigative support to trial counsel during the judicial process.                                                                                         |          |         |                    |               |               |                               | 1               | 1          | 1         | 3                | 3            |               |               |               |               |
| Analyze computer-generated threats for counter intelligence or criminal activity.                                                                                            |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 1            |               |               |               |               |
| Construct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.        |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Determine and develop leads and identify sources of information to identify and/or prosecute the responsible parties to an intrusion or other crimes.                        |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Create documentation of original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking).                   |          |         |                    |               |               |                               | 3               | 2          | 2         | 1                | 2            |               |               |               |               |
| Employ IT systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property.                             |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |
| Prepare reports to document the investigation following legal standards and requirements.                                                                                    |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |
| Analyze incident data for emerging trends.                                                                                                                                   |          |         |                    |               |               |                               | 1               | 2          | 2         | 3                | 3            |               |               |               |               |
| Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.                                                                 |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 1            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                                                                                                                                | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.                                                                                                                                               |          |         |                    |               |               |                               | 2               | 2          | 2         | 2                | 2            |               |               |               |               |
| Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).                                                                             |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Create and/or apply reverse engineering tools to enhance capabilities and detect vulnerabilities.                                                                                                                                                                                                                           |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 1            |               |               |               |               |
| Analyze organizational cyber policy.                                                                                                                                                                                                                                                                                        |          |         |                    |               |               |                               | 1               | 2          | 2         | 2                | 3            |               |               |               |               |
| Assess and confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.                                                                                                                                                                            |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 1            |               |               |               |               |
| Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats. |          |         |                    |               |               |                               | 3               | 3          | 2         | 1                | 2            |               |               |               |               |
| Apply skills in decrypting seized data using technical means.                                                                                                                                                                                                                                                               |          |         |                    |               |               |                               |                 | 1          | 1         | 0                | 1            |               |               |               |               |
| Compose technical summaries of findings in accordance with established reporting procedures.                                                                                                                                                                                                                                |          |         |                    |               |               |                               | 3               | 3          | 3         | 2                | 2            |               |               |               |               |
| Demonstrate that chain of custody is followed for all digital media acquired in accordance with the existing code of conduct.                                                                                                                                                                                               |          |         |                    |               |               |                               | 3               | 3          | 2         | 3                | 3            |               |               |               |               |
| Perform dynamic analysis to boot an "image" of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment.                                                                                                                                          |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 1            |               |               |               |               |
| Perform file signature analysis.                                                                                                                                                                                                                                                                                            |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 1            |               |               |               |               |
| Perform hash comparison against established database.                                                                                                                                                                                                                                                                       |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 1            |               |               |               |               |
| Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView or Kali).                                                                                                                                                                                                                               |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 1            |               |               |               |               |
| Perform Timeline Analysis and Data Correlation and point out relationships between findings                                                                                                                                                                                                                                 |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 1            |               |               |               |               |
| Perform real-time incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis) tasks to support deployable Rapid Response Teams (RRTs).                                                                                                                                              |          |         |                    |               |               |                               | 0               | 1          | 2         | 1                | 1            |               |               |               |               |
| Set-up digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).                                                                                                                                                                                        |          |         |                    |               |               |                               | 3               | 2          | 2         | 1                | 1            |               |               |               |               |
| Organize technical assistance on digital evidence matters to appropriate personnel.                                                                                                                                                                                                                                         |          |         |                    |               |               |                               | 2               | 2          | 2         | 3                | 3            |               |               |               |               |
| Recognize and accurately report forensic artifacts indicative of a particular operating system.                                                                                                                                                                                                                             |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).                                                                                                                                                                                                                                       |          |         |                    |               |               |                               | 3               | 3          | 2         | 1                | 1            |               |               |               |               |
| Capture and analyze network traffic associated with malicious activities using network monitoring tools.                                                                                                                                                                                                                    |          |         |                    |               |               |                               | 3               | 2          | 2         | 1                | 1            |               |               |               |               |
| Operate as technical expert and liaison to law enforcement personnel and explain incident details as required.                                                                                                                                                                                                              |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Perform virus scanning on digital media.                                                                                                                                                                                                                                                                                    |          |         |                    |               |               |                               | 3               | 2          | 2         | 1                | 1            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                               | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Perform file system forensic analysis.                                                                                                                                                                     |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 1            |               |               |               |               |
| Perform static malware analysis.                                                                                                                                                                           |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 1            |               |               |               |               |
| Utilize deployable forensics toolkit to support operations as necessary.                                                                                                                                   |          |         |                    |               |               |                               | 3               | 3          | 2         | 1                | 1            |               |               |               |               |
| Coordinate with intelligence analysts to correlate threat assessment data.                                                                                                                                 |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 1            |               |               |               |               |
| Process image with appropriate tools depending on analyst's goals.                                                                                                                                         |          |         |                    |               |               |                               | 3               | 3          | 2         | 1                | 1            |               |               |               |               |
| Perform Windows registry analysis.                                                                                                                                                                         |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 1            |               |               |               |               |
| Enter media information into tracking database (e.g., Product Tracker Tool) for digital media that has been acquired.                                                                                      |          |         |                    |               |               |                               | 3               | 2          | 2         | 1                | 1            |               |               |               |               |
| Correlate incident data and perform cyber defense reporting.                                                                                                                                               |          |         |                    |               |               |                               | 1               | 2          | 1         | 3                | 2            |               |               |               |               |
| Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.    |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.                                                                                      |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 1            |               |               |               |               |
| Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.                                                                             |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Identify and determine which ISO standards have to be taken account in which investigative action.                                                                                                         |          |         |                    |               |               |                               | 1               | 2          | 2         | 2                | 3            |               |               |               |               |
| Describe the legal acts which allow you to conduct investigations                                                                                                                                          |          |         |                    |               |               |                               | 1               | 2          | 2         | 2                | 3            |               |               |               |               |
| <b>Tier 6: Digital Forensics Speciality Knowledge Competencies</b>                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Digital Forensic Technology: The knowledge, skills, and abilities needed to understand the purpose and function of forensic technology, including tools and systems.</b>                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Knowledge areas</b>                                                                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Be familiar with VMware and be able to import and configure virtual machines.                                                                                                                              |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Have a general idea about core programming concepts such as variables, loops, and functions in order to quickly grasp the relevant concepts in this area; however, no programming experience is necessary. |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Describe computer networking concepts and protocols, and network security methodologies.                                                                                                                   |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Describe risk management processes (e.g., methods for assessing and mitigating risk).                                                                                                                      |          |         |                    |               |               |                               | 1               | 2          | 2         | 2                | 2            |               |               |               |               |
| Recall laws, regulations, policies, and ethics related to cyber incident investigations and privacy.                                                                                                       |          |         |                    |               |               |                               | 2               | 2          | 2         | 2                | 3            |               |               |               |               |
| Identify cybersecurity and privacy principles.                                                                                                                                                             |          |         |                    |               |               |                               | 2               | 3          | 3         | 3                | 3            |               |               |               |               |
| List specific operational impacts of cybersecurity lapses.                                                                                                                                                 |          |         |                    |               |               |                               | 1               | 2          | 2         | 3                | 3            |               |               |               |               |
| Name intrusion detection methodologies and techniques for detecting host and network-based intrusions.                                                                                                     |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Describe Insider Threat investigations, reporting, investigative tools and laws/regulations.                                                                                                               |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                              | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Name and describe processes for seizing and preserving digital evidence.                                                                                                                                                  |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |
| Name legal governance related to admissibility (e.g. Rules of Evidence in Code of Criminal Procedure)                                                                                                                     |          |         |                    |               |               |                               |                 |            | 3         |                  | 3            |               |               |               |               |
| List types and collection of persistent data.                                                                                                                                                                             |          |         |                    |               |               |                               | 2               | 2          | 2         | 1                | 2            |               |               |               |               |
| Give examples for use of electronic evidence law.                                                                                                                                                                         |          |         |                    |               |               |                               | 2               | 2          | 3         | 3                | 3            |               |               |               |               |
| Name and explain applicable laws, statutes (e.g., in § 124, and 211 in Estonian Code of Criminal Procedure and), Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures. |          |         |                    |               |               |                               | 2               | 2          | 3         | 3                | 3            |               |               |               |               |
| Observe for physical and physiological behavior patterns that may indicate suspicious or abnormal activity.                                                                                                               |          |         |                    |               |               |                               | 1               | 1          | 2         | 1                | 2            |               |               |               |               |
| Describe the judicial process, including the presentation of facts and evidence.                                                                                                                                          |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 3            |               |               |               |               |
| Relate to applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.                                                                                                                 |          |         |                    |               |               |                               | 1               | 1          | 2         | 2                | 3            |               |               |               |               |
| Application Security Risks (e.g. Open Web Application Security Project Top 10 list)                                                                                                                                       |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Name the latest concepts and practices of processing digital forensic data.                                                                                                                                               |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Name incident response and handling methodologies.                                                                                                                                                                        |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |
| List server diagnostic tools and fault identification techniques and give examples for their uses.                                                                                                                        |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Give descriptive summarize of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).                                                                   |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Name and describe hacking methodologies.                                                                                                                                                                                  |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| List web mail collection, searching/analyzing techniques, tools, and cookies.                                                                                                                                             |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Name which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.                                                                         |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Name and describe types of digital forensics data and how to recognize them.                                                                                                                                              |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 3            |               |               |               |               |
| Name system administration, network, and operating system hardening techniques.                                                                                                                                           |          |         |                    |               |               |                               | 2               | 3          | 3         | 3                | 3            |               |               |               |               |
| Describe network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).                                                                        |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| List reverse engineering concepts.                                                                                                                                                                                        |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Utilize forensics lab design configuration and support applications (e.g., VMWare, Wireshark).                                                                                                                            |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Name debugging procedures and tools.                                                                                                                                                                                      |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Define file type abuse by adversaries for anomalous behavior.                                                                                                                                                             |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Classify malware analysis tools (e.g., Oily Debug, Ida Pro).                                                                                                                                                              |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Distinguish malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer's display device).                        |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                                                                                                      | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Be able to recognize data concealment (e.g. encryption algorithms and steganography).                                                                                                                                                                                                             |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Describe and give examples to encryption algorithms.                                                                                                                                                                                                                                              |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Give examples to system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).                                                                                                                                         |          |         |                    |               |               |                               |                 |            | 3         |                  | 2            |               |               |               |               |
| Explain binary analysis.                                                                                                                                                                                                                                                                          |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Explain network architecture concepts including topology, protocols, and components.                                                                                                                                                                                                              |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Describe packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).                                                                                                                                                                                                                |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Express knowledge and understanding of organizations operational design.                                                                                                                                                                                                                          |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |
| <b>Skills:</b>                                                                                                                                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate skill in preserving evidence integrity according to standard operating procedures or national standards.                                                                                                                                                                              |          |         |                    |               |               |                               | 3               | 2          | 3         | 1                | 2            |               |               |               |               |
| Apply physical and e-evidence collecting, processing, packaging, transporting, and storing to avoid alteration, loss, physical damage, or destruction of data.                                                                                                                                    |          |         |                    |               |               |                               | 3               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).                                                                                                                                                                                                                 |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Analyze malware.                                                                                                                                                                                                                                                                                  |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Illustrate skill in conducting bit-level analysis.                                                                                                                                                                                                                                                |          |         |                    |               |               |                               |                 |            | 3         |                  | 2            |               |               |               |               |
| Perform digital evidence processing to include protecting and making legally sound copies of evidence.                                                                                                                                                                                            |          |         |                    |               |               |                               | 3               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform packet-level analysis.                                                                                                                                                                                                                                                                    |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Detect how and when a breach occurred                                                                                                                                                                                                                                                             |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Identify compromised and affected systems                                                                                                                                                                                                                                                         |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform damage assessments and determine what was stolen or changed                                                                                                                                                                                                                               |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Contain and remediate incidents                                                                                                                                                                                                                                                                   |          |         |                    |               |               |                               | 1               | 3          | 3         | 2                | 2            |               |               |               |               |
| Develop key sources of threat intelligence                                                                                                                                                                                                                                                        |          |         |                    |               |               |                               |                 |            | 2         |                  | 2            |               |               |               |               |
| Hunt down additional breaches using knowledge of the adversary                                                                                                                                                                                                                                    |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Assist Law Enforcement in Evidence Collection Procedures                                                                                                                                                                                                                                          |          |         |                    |               |               |                               | 3               | 1          | 2         | 1                | 2            |               |               |               |               |
| Know How To Keep Evidence Integrity                                                                                                                                                                                                                                                               |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |
| Presentation and Reporting of Evidence and Analysis                                                                                                                                                                                                                                               |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                  | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-----------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Perform Windows OS Investigation and Analysis                                                 |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Unix based OS Investigation and Analysis                                              |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Windows In-Depth Registry Forensics                                                   |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 1            |               |               |               |               |
| Track User Activity                                                                           |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| <b>Abilities:</b>                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Ability to find and navigate the dark web using the TOR network to locate markets and forums. |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Ability to examine digital media on multiple operating system platforms.                      |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Ability to decrypt digital data collections.                                                  |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Ability to conduct forensic analyses in Windows environments.                                 |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Ability to conduct forensic analyses in Unix/Linux environments.                              |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Participate in Digital Forensic Case                                                          |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |
| <b>Tier 7: Digital Forensics Standard-Specific Competencies</b>                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>The knowledge and skills needed stay proficient in DF subdivisions</b>                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>0.1 Computer Forensics</b>                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Describe Investigative Methodologies                                                          |          |         |                    |               |               |                               | 1               | 3          | 3         | 2                | 3            |               |               |               |               |
| Use Ubuntu SIFT, Kali and Windows Workstations                                                |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Describe The Volatility Framework                                                             |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Understand the System Architectures                                                           |          |         |                    |               |               |                               | 3               | 3          | 3         | 2                | 2            |               |               |               |               |
| Describe the difference between Triage versus Full Memory Acquisition                         |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |
| Perform Physical Memory Acquisition                                                           |          |         |                    |               |               |                               | 3               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Unstructured Memory Analysis                                                          |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Page File Analysis                                                                    |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Describe the Exploring Process Structures                                                     |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Describe the difference Walking and Scanning method                                           |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Describe the Process Relationships                                                            |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Be able to associate DLLs with processes and describe the relationships                       |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Understand and describe process specific Kernel Objects                                       |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                          | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|---------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| List different Network Connections                                                    |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Understand the concept Virtual Address Descriptors                                    |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Detect Injected Code                                                                  |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze the Registry via Memory Analysis                                              |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Memory, Pagefile, and Unallocated Artifact Carving                            |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Detect User Artifacts in Memory                                                       |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Interrupt Descriptor Tables                                                           |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Describe the use of System Service Descriptor Tables                                  |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Illustrate the use of Drivers and Driver analysis                                     |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Conduct and detect Direct Kernel Object Manipulation                                  |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Module Extraction                                                             |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze Hibernation Files                                                             |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze Crash Dump Files                                                              |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Linux Memory Acquisition and Analysis                                         |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Mac Memory Acquisition and Analysis                                           |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Malware and Rootkit Behavior Detection                                        |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Identify Persistence Mechanism                                                        |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Code Injection Analysis                                                       |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Reconstruct User Activity                                                             |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Linux Memory Image Parsing                                                    |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Mac OSX Memory Image Parsing                                                  |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Conduct Windows Hibernation File Conversion and Analysis                              |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Windows Crash Dump Analysis (Using Windows Debugger)                          |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Conduct cursory binary analysis                                                       |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| <b>0.2 Software Forensics</b>                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand and describe the use of different Windows Operating System Components      |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 3            |               |               |               |               |
| Describe and be able do perform Live Response and Triage-Based Acquisition Techniques |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                        | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Perform Acquisition Review with Write Blocker                                                                                                                                                       |          |         |                    |               |               |                               | 3               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Windows Image Mounting and Examination on a monthly/weekly bases                                                                                                                            |          |         |                    |               |               |                               | 2               | 3          | 1         | 1                | 1            |               |               |               |               |
| Give overview NTFS File System                                                                                                                                                                      |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Conduct File Carving                                                                                                                                                                                |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Search for Custom Carving Signatures                                                                                                                                                                |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 1            |               |               |               |               |
| Perform Memory, Pagefile, and Unallocated Space Analysis                                                                                                                                            |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Understand Registry Basics                                                                                                                                                                          |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |
| Analyze Profile Users and Groups (e.g Access Rights)                                                                                                                                                |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Identify and describe Core System Information                                                                                                                                                       |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Identify User Forensic Data                                                                                                                                                                         |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Shell Item Forensics                                                                                                                                                                        |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Email Forensics                                                                                                                                                                             |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Windows Event Log Analysis                                                                                                                                                                  |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Browser Forensics: History, Cache, Searches, Downloads, Understanding of Browser Timestamps, (e.g.Internet Explorer, Firefox, Chrome, Safari, Opera, Microsoft, Netscape, Sleipnir, Comodo) |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Name the Tools Used                                                                                                                                                                                 |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Distinguish Mac and Apple Essentials and Acquisition procedures                                                                                                                                     |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Describe the different Disks & Partitions possibilities                                                                                                                                             |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform iOS Acquisition                                                                                                                                                                             |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Practice doing iOS Backups                                                                                                                                                                          |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Describe the HFS+ File System                                                                                                                                                                       |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Name iOS Extended Attributes                                                                                                                                                                        |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Describe the File System Events Store Database                                                                                                                                                      |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Describe what is Spotlight                                                                                                                                                                          |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Explain what are Portable Artifacts                                                                                                                                                                 |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Conduct Mac and iOS Triage                                                                                                                                                                          |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Be familiar with term Most Recently Used (MRU)                                                                                                                                                      |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Find and Identify User Data and System Configuration                                                                                                                                                |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                         | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|--------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Perform Log Parsing and Analysis                                                                                                     |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Observe Application Permissions                                                                                                      |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| List Native Applications                                                                                                             |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Describe what are the specifics about Apple Mail                                                                                     |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Apple Watch forensics                                                                                                        |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| List Third-Party Apps                                                                                                                |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Conduct Live Response forensics                                                                                                      |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Time Machine and Time Capsule forensics                                                                                      |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform OS X Malware and Intrusion Analysis                                                                                          |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform iCloud forensics                                                                                                             |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Memory Acquisitions and Analysis                                                                                             |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Describe and make use of Password Cracking and Encrypted Containers                                                                  |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Mac Memory Analysis                                                                                                          |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Conduct File System Data Analysis                                                                                                    |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Demonstrate skills in Recovering Key Mac Files                                                                                       |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Volume and Disk Image Analysis                                                                                               |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Conduct Analysis of Mac Technologies including Time Machine, Spotlight, and FileVault                                                |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform iDevice Analysis and iOS Artifacts                                                                                           |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Assembling a Toolkit for Effective Malware Analysis                                                                                  |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Examine Static Properties of Suspicious Programs                                                                                     |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Behavioral Analysis of Malicious Windows Executables                                                                         |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Static and Dynamic Code Analysis of Malicious Windows Executables                                                            |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Interact with Malware in a Lab conditions to Derive Additional Behavioral Characteristics                                            |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Understand Core x86 Assembly Concepts to Perform Malicious Code Analysis                                                             |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Identify Key Assembly Logic Structures by making use of a Disassembler                                                               |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Follow Program Control Flow to Understand Decision Points During Execution                                                           |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Recognize Common Malware Characteristics at the Windows API Level (Registry Manipulation, Keylogging, HTTP Communications, Droppers) |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                         | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|--------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Perform Code Assembly in x64 Code Analysis                                           |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Interact with Malicious Websites to Assess the Nature of Their Threats               |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| De-obfuscate Malicious JavaScript Using Debuggers and Interpreters                   |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Examine Malicious Microsoft Office Documents, Including Files with Macros            |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze Malicious RTF Document Files                                                 |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Recognize Packed Malware                                                             |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Use Debuggers for Dumping Packed Malware from Memory                                 |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze Multi-Technology and Fileless Malware                                        |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Code Injections and API Hooking                                              |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Use Memory Forensics for Malware Analysis                                            |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze Malicious Microsoft Office (Word, Excel, PowerPoint) Documents               |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze Malicious Adobe PDF Documents                                                |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze Memory to Assess Malware Characteristics and Reconstruct Infection Artifacts |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Use Memory Forensics to Analyze Rootkit Infections                                   |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Conduct Behavioral Malware Analysis                                                  |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Conduct Dynamic Malware Analysis (Using a Debugger)                                  |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Conduct Static Malware Analysis (Using a Disassembler)                               |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform JavaScript Deobfuscation                                                     |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Facebook, Gmail, Hotmail, Yahoo Chat and Webmail Analysis                    |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform E-mail Forensics (Host, Server, Web)                                         |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Windows Link File Investigation                                              |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Windows Recycle Bin Analysis                                                 |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform File and Picture Metadata Tracking and Examination                           |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Firefox and Internet Explorer Browser Forensics                              |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform InPrivate Browsing Recover                                                   |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Deleted File Recovery                                                        |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform String Searching and Data Carving                                            |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| <b>0.3 Database Forensics</b>                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Create a forensic copy of a database for analysis                                                           |          |         |                    |               |               |                               | 3               | 2          | 3         | 1                | 2            |               |               |               |               |
| Reconstruct missing data and/or log files associated with the deletion                                      |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Decipher data and ascertain possible causes of corruption                                                   |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Audit user activities and isolate suspicious and illegal behavior                                           |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Conduct analysis of Oracle                                                                                  |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Conduct analysis of MySQL                                                                                   |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Conduct analysis of Microsoft SQL Server                                                                    |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Conduct analysis of PostgreSQL                                                                              |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Conduct analysis of MongoDB                                                                                 |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| <b>0.4 Multimedia Forensics</b>                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Understand various modalities of device fingerprints                                                        |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Describe ways for extracting and enhancing device fingerprints from digital content                         |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Understand forensic applications of device fingerprints in source device identification                     |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform content/device linking                                                                              |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform source-oriented image clustering and content integrity verification                                 |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Understand data hiding techniques and their applications in copyright protection and content authentication |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Understand data hiding techniques and their applications in steganography and steganalysis                  |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Understand theoretical and practical challenges, including counter-forensics and counter-counter-forensics  |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Digital content hashing                                                                             |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Communication App forensics                                                                         |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze Calendar and Reminder Apps                                                                          |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze Contact managing Apps                                                                               |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze Notes and List Apps                                                                                 |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze Photo Apps                                                                                          |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze Map and Sporting Apps                                                                               |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Analyze and connect Location Data to findings                                                               |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                      | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|---------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Perform Metadata analysis                                                                         |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Facebook, Gmail, Hotmail, Yahoo Chat and Webmail Analysis                                 |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform E-mail Forensics (Host, Server, Web)                                                      |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Microsoft Office Document Analysis                                                        |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Windows Link File Investigation                                                           |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Windows Recycle Bin Analysis                                                              |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform File and Picture Metadata Tracking and Evaluation                                         |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Firefox and Internet Explorer Browser Forensics                                           |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform InPrivate Browsing Recover                                                                |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Deleted File Recovery                                                                     |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform static media analysis.                                                                    |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| <b>0.5 Device Forensics</b>                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Perform USB Device Tracking and Analysis                                                          |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Make use of SIFT Workstation                                                                      |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Describe Malware and Spyware effects on different devices. Analyze and share the latest findings. |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Perform Smartphone Handling                                                                       |          |         |                    |               |               |                               | 3               | 2          | 3         | 1                | 2            |               |               |               |               |
| Describe the Forensic Acquisition Concepts of Smartphones                                         |          |         |                    |               |               |                               | 3               | 3          | 3         | 2                | 2            |               |               |               |               |
| Give the Smartphone Forensics Tool's Overview                                                     |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Apply JTAG(Joint Test Action Group) Forensics                                                     |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Name Smartphone Components                                                                        |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Illustrate SQLite usages on different devices                                                     |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Give Android Forensics Overview in for insight on compiling internal course material              |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Demonstrate know-how and skills on Handling Locked Android Devices                                |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Android File System Structures                                                                    |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Android Evidentiary Locations                                                                     |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Observe Traces of User Activity on Android Devices                                                |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Produce and Analyze Android Backup Files                                                          |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                 | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|----------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Identify different iOS Forensics and Acquisition Methods                                     |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Name iOS File System Structures                                                              |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Name iOS Evidentiary Locations                                                               |          |         |                    |               |               |                               | 1               | 3          | 3         | 1                | 2            |               |               |               |               |
| Demonstrate know-how and skills on Handling Locked iOS Devices                               |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Observe Traces of User Activity on iOS Devices                                               |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Produce and Analze iOS Backup Files                                                          |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Windows Phone/Mobile Forensics                                                       |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform BlackBerry Forensics (File System, Evidentiary Locations, and Forensic Analysis      |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Name BlackBerry File System Structures                                                       |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Name BlackBerry Evidentiary Locations                                                        |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Demonstrate know-how and skills on Handling Locked BlackBerry Devices                        |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Observe Traces of User Activity on BlackBerry Devices                                        |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| List Third-Party Applications, Artifacts. Describe latest vulnerabilites and security issues |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| List Messaging Applications                                                                  |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Recover Attachments from Messaging Applications                                              |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| List and Describe the Different Secure Chat Applications.                                    |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| List the Security Issues and Vulnerabilities of Different Mobile Browsers                    |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Perform Knock-off Phone Forensics                                                            |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| <b>0.6 Network Forensics</b>                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Perform Access Control and Password Management                                               |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Observe for Malicious Code and Exploit Mitigations                                           |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Describe Advanced Persistent Threat (APT)                                                    |          |         |                    |               |               |                               | 2               | 3          | 3         | 3                | 3            |               |               |               |               |
| List number of Critical Controls                                                             |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| Manage Security Policies                                                                     |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| List Key Infrastructure Devices                                                              |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Describe The Concept of Segmented Internal Networks                                          |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |
| Describe Defensible Network Security Architecture Principles                                 |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                         | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|----------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Describe Core Protocols & Log Aggregation/Analysis                   |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Describe Hypertext Transfer Protocol (HTTP): Protocol and Logs       |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Describe Domain Name Service (DNS): Protocol and Logs                |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Describe Cloud Security: In-House versus Cloud                       |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| A Virtualization Security Primer                                     |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| Cloud Network Security                                               |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| Describe Instance and Image Security                                 |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| Data Security for the Cloud                                          |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| Application Security for the Cloud                                   |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| Provider Security: Cloud Risk Assessment                             |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Identity and Access Management                                       |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| Use Network Forensics Tools: tcpdump and Wireshark                   |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Perform Network Evidence Acquisition                                 |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| Identify Network Architectural Challenges and Opportunities          |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Understand and identify the common types of attacks against networks |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |
| Describe Logging Protocol and Aggregation                            |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Describe ELK Stack and the SOF-ELK Platform                          |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| Perform NetFlow Collection and Analysis                              |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| List Open-Source Flow Tools                                          |          |         |                    |               |               |                               | 3               | 3          | 3         | 2                | 2            |               |               |               |               |
| Describe File Transfer Protocol (FTP)                                |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Describe Microsoft Protocols                                         |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Describe Simple Mail Transfer Protocol (SMTP)                        |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Name and Make Use of Commercial Network Forensics Tools              |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |
| Perform Wireless Network Forensics                                   |          |         |                    |               |               |                               | 3               | 3          | 3         | 1                | 2            |               |               |               |               |
| List Automated Tools and Libraries                                   |          |         |                    |               |               |                               | 2               | 3          | 3         | 1                | 2            |               |               |               |               |
| Describe and Make use of Full-Packet Hunting with Moloch             |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Describe Encoding, Encryption, and SSL                               |          |         |                    |               |               |                               | 2               | 3          | 3         | 2                | 2            |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                      | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Describe Man in the Middle Concept                                                                                                                                                |          |         |                    |               |               |                               | 3               | 3          | 3         | 3                | 3            |               |               |               |               |
| Perform Network Protocol Reverse Engineering                                                                                                                                      |          |         |                    |               |               |                               | 1               | 2          | 3         | 1                | 2            |               |               |               |               |
| Investigation OPSEC and Threat Intel                                                                                                                                              |          |         |                    |               |               |                               | 2               | 2          | 3         | 1                | 2            |               |               |               |               |
| Have insight in the realities of modern Bluetooth security challenges and vulnerabilities                                                                                         |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| Describe and compare the use benefits in different Bluetooth tool (e.g Btlejuice, BlueHydra, L2ping command within the Linux Bluez library)                                       |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| Revise and build internal policies to ensure cloud security is properly addressed                                                                                                 |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Understand all major facets of cloud risk, including threats, vulnerabilities, and impact                                                                                         |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Articulate the key security topics and risks associated with SaaS, PaaS, and IaaS cloud deployment models                                                                         |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Evaluate Cloud Access Security Brokers (CASBs) to better protect and monitor SaaS deployments                                                                                     |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Build security for all layers of a hybrid cloud environment, starting with hypervisors and working to application layer controls                                                  |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Evaluate basic virtualization hypervisor security controls                                                                                                                        |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| Design and implement network security access controls and monitoring capabilities in a public cloud environment                                                                   |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Design a hybrid cloud network architecture that includes IPSec tunnels                                                                                                            |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Integrate cloud identity and access management (IAM) into security architecture                                                                                                   |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Evaluate and implement various cloud encryption types and formats                                                                                                                 |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Develop multi-tier cloud architectures in a Virtual Private Cloud (VPC), using subnets, availability zones, gateways, and NAT                                                     |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Integrate security into DevOps teams, effectively creating a DevSecOps team structure                                                                                             |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Build automated deployment workflows using AWS and native tools                                                                                                                   |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Incorporate vulnerability management, scanning, and penetration testing into cloud environments                                                                                   |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Build automated and flexible detection and response programs using tools like AWS-IR, CloudWatch, CloudTrail, and AWS Lambda                                                      |          |         |                    |               |               |                               | 1               | 2          | 3         | 2                | 2            |               |               |               |               |
| Leverage the AWS CLI to automate and easily execute operational tasks                                                                                                             |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| Set up and use an enterprise automation platform, Ansible, to automate configuration and orchestration tasks                                                                      |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| Use CloudWatch, CloudFormation, and other automation tools to integrate automated security controls into your cloud security program                                              |          |         |                    |               |               |                               | 2               | 2          | 3         | 2                | 2            |               |               |               |               |
| <b>Tier 8: Digital Forensics Specific Roles</b>                                                                                                                                   |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Responsive: Roles responsible for rapid reaction units to distant locations and investigating incidents on IT systems, networks regarding of electronic(digital) evidence.</b> |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| <b>Incident Response Team / Rapid Reaction Team</b>                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Cyber Crime Investigator                                                                                                                                                    |          |         |                    | x             |               |                               |                 |            |           |                  |              |               |               |               |               |
| Incident Handler                                                                                                                                                            |          |         |                    |               | x             |                               |                 |            |           |                  |              |               |               |               |               |
| 1st line - data collection and basic analysis                                                                                                                               |          |         |                    |               | x             |                               |                 |            |           |                  |              |               |               |               |               |
| Incident Response Analyst                                                                                                                                                   |          |         |                    |               | x             |                               |                 |            |           |                  |              |               |               |               |               |
| Digital Forensics Expert                                                                                                                                                    |          |         |                    |               | x             |                               |                 |            |           |                  |              |               |               |               |               |
| Intrusion Analyst                                                                                                                                                           |          |         |                    | x             |               |                               |                 |            |           |                  |              |               |               |               |               |
| Team leader / manager                                                                                                                                                       |          |         |                    |               | x             |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Investigative: Roles responsible for investigating cyber events or crimes of information technology (IT) systems, networks, and electronic(digital) evidence.</u></b> |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Digital Forensics</b>                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Computer Forensic Expert Analyst                                                                                                                                            |          |         |                    |               | x             |                               |                 |            |           |                  |              |               |               |               |               |
| Software Forensic Expert Analyst                                                                                                                                            |          |         |                    |               | x             |                               |                 |            |           |                  |              |               |               |               |               |
| Database Forensic Expert Analyst                                                                                                                                            |          |         |                    |               | x             |                               |                 |            |           |                  |              |               |               |               |               |
| Network Forensic Expert Analyst                                                                                                                                             |          |         |                    |               | x             |                               |                 |            |           |                  |              |               |               |               |               |
| Digital Media Collector                                                                                                                                                     |          |         |                    |               | x             |                               |                 |            |           |                  |              |               |               |               |               |
| Forensic Analyst                                                                                                                                                            |          |         |                    | x             |               |                               |                 |            |           |                  |              |               |               |               |               |
| Forensic Analyst (Cryptologic)                                                                                                                                              |          |         |                    | x             |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Cyber Investigation</b>                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Cyber Crime Investigator                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| e-police                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Vulnerability Assessment and Management</b>                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Blue Team Technician                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Certified TEMPEST Professional                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Certified TEMPEST Technical Authority                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Close Access Technician                                                                                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Computer Network Defense (CND) Auditor                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Compliance Manager                                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                               | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Ethical Hacker                                                                                                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Governance Manager                                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Information Security Engineer                                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Internal Enterprise Auditor                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Penetration Tester                                                                                                                                                                         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Red Team Technician                                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Network Security Engineer                                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Reverse Engineer                                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Risk/Vulnerability Analyst                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Technical Surveillance Countermeasures Technician                                                                                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Vulnerability Manager                                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Intelligence collection: Roles responsible for information collection for cybersecurity means that may be used for investigations.</u></b>                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Intelligence Analyst                                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Counter-Intelligence Analyst                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Analyze Information: Is responsible for highly specialized review and evaluation of incoming cybersecurity related information to determine its usefulness for intelligence.</u></b> |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Intelligence Analyst                                                                                                                                                                       |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Counter-Intelligence Analyst                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b><u>Overseeing, Governance and Aid: responsible for providing management, guidance and development for the organization to work effectively.</u></b>                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Legal Advice and Advocacy</b>                                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Legal Advisor (LEGAD)                                                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Paralegal                                                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Prosecutor's Office                                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Strategic Planning and Policy Development</b>                                                                                                                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Chief Information Officer (CIO)                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Chief Information Security Officer (CISO)                                                                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Command Information Officer                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                                                                                                                               | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Information Security Policy Analyst                                                                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Information Security Policy Manager                                                                                                                                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Policy Writer and Strategist                                                                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Training, Education</b>                                                                                                                                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Personal management planner                                                                                                                                                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Trainer                                                                                                                                                                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Information Security Trainer                                                                                                                                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Forensic Training Coordinator                                                                                                                                                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| <b>Tier 9 Digital Forensic Specialist Specific Requirements</b>                                                                                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Demonstrate sufficient knowledge and experience in the field of expertise (Digital Forensic subdivision)                                                                                                                                   |          |         |                    |               |               |                               |                 | 2          | 2         |                  |              |               |               |               |               |
| Express 3 years of relevant work experience at the level of an academic Master's Degree preferably in the field of technical IT                                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Express at least 5 years of relevant work experience at the level of an academic Bachelor's Degree preferably in the field of technical IT                                                                                                 |          |         |                    |               |               |                               |                 | 1          | 1         |                  |              |               |               |               |               |
| Recognize the summary of concepts (see Tiers 6 - 8) and keep abreast of state of the art developments                                                                                                                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| List up to date technological and other developments in the field and taking active steps to maintain competence                                                                                                                           |          |         |                    |               |               |                               |                 | 1          | 1         |                  |              |               |               |               |               |
| Name the fundamental principles of forensic investigations (e.g. crime scene investigation, chain of custody, principles of evidence)                                                                                                      |          |         |                    |               |               |                               |                 | 2          | 2         |                  |              |               |               |               |               |
| Demonstrate adequate knowledge of the collection, examination and analysis of data.                                                                                                                                                        |          |         |                    |               |               |                               |                 | 2          | 2         |                  |              |               |               |               |               |
| Demonstrate at least 5 incident investigation reports not older than 5 years which have been subjected to review                                                                                                                           |          |         |                    |               |               |                               |                 | 2          | 2         |                  |              |               |               |               |               |
| Demonstrate an average of 40 hours a year on forensically relevant professional development (e.g. attending conferences, running or attending courses, exercises, competitions, workshops, publications)                                   |          |         |                    |               |               |                               |                 | 1          | 1         |                  |              |               |               |               |               |
| Inform the commissioning party whether, and if so, to what extent the commissioning party's question at issue is sufficiently clear and capable of investigation in order to be able to answer it on the basis of their specific expertise |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Prepare and carry out an investigation plan in accordance with the applicable standards                                                                                                                                                    |          |         |                    |               |               |                               |                 | 1          | 1         |                  |              |               |               |               |               |
| Demonstrate skills to collect, document, interpret and assess investigative materials and data in a forensic context in accordance with the applicable standards                                                                           |          |         |                    |               |               |                               |                 | 2          | 2         |                  |              |               |               |               |               |
| Apply the current investigative methods in a forensic context in accordance with the applicable standards                                                                                                                                  |          |         |                    |               |               |                               |                 | 1          | 1         |                  |              |               |               |               |               |
| Be able to compose both orally and in writing, a verifiable and well-reasoned report on the assignment and any other relevant aspects of their expertise in terms which are comprehensible to the commissioning party                      |          |         |                    |               |               |                               |                 | 1          | 1         |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                                | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-----------------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Schedule assignments timeframe accordingly within the stipulated or agreed period                                           |          |         |                    |               |               |                               |                 | 1          | 1         |                  |              |               |               |               |               |
| Conduct the activities as an expert independently, impartially, conscientiously, competently, and in a trustworthy manner.  |          |         |                    |               |               |                               |                 | 2          | 2         |                  |              |               |               |               |               |
| <b>Tier 10 Digital Forensic Management Competencies</b>                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Make sense of different cybersecurity frameworks                                                                            |          |         |                    |               |               |                               |                 | 1          | 1         |                  |              |               |               |               |               |
| Understand and analyze risk                                                                                                 |          |         |                    |               |               |                               |                 | 1          | 1         |                  |              |               |               |               |               |
| Understand the pros and cons of different reporting relationships                                                           |          |         |                    |               |               |                               |                 | 1          | 1         |                  |              |               |               |               |               |
| Manage technical personnel                                                                                                  |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Build a vulnerability management program                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Inject security into modern DevOps workflows                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Strategically leverage a SIEM                                                                                               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Change behavior and build a security-aware society                                                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Effectively manage security projects                                                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Develop security strategic plans                                                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Develop and assess information security policy                                                                              |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Use management and leadership techniques to motivate and inspire your teams                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Recognize the top failure mechanisms related to IT and infosec projects, so that your projects can avoid common pitfalls    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Create a project charter which defines the project sponsor and stakeholder involvement                                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Document project requirements and create requirements traceability matrix to track changes throughout the project lifecycle |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Clearly define the scope of a project in terms of cost, schedule and technical deliverables                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Create a work breakdown structure defining work packages, project deliverables and acceptance criteria                      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Develop a detailed project schedule, including critical path tasks and milestones                                           |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Develop a detailed project budget including cost baselines and tracking mechanisms                                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Effectively manage conflict situations and build communication skills with your project team                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Document project risks in terms of probability and impact, assign triggers and incident risk response responsibilities      |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Creating Incident Response Requirements                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |

**Annex VIII: Digital Forensics Workforce Competency Model (adapted from Competency Models for Enterprise Security and Cybersecurity, 2015).**

| Competencies                                                                                                          | Achieved | Desired | Not Applicable (1) | Preferred (2) | Essential (3) | Recruitment Requirement (Y/N) | First Responder | DF Analyst | DF Expert | Incident Handler | Team Manager | Course plan 1 | Course plan 2 | Course plan 3 | Course plan 4 |
|-----------------------------------------------------------------------------------------------------------------------|----------|---------|--------------------|---------------|---------------|-------------------------------|-----------------|------------|-----------|------------------|--------------|---------------|---------------|---------------|---------------|
| Developing Incident Handling Capabilities                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Reporting, SLAs, Cost of Incidents                                                                                    |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Setting up Operations                                                                                                 |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Managing Daily Operations                                                                                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Observe for Advanced Persistent Threat                                                                                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Solve Legal and Regulatory Issues                                                                                     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Work with other departments at your organization who make decisions about the law of data security and investigations |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Exercise better judgment on how to comply with technology regulations, both in Estonia and in other countries         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Evaluate the role and meaning of contracts for technology, including services, software and outsourcing               |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Help your organization better explain its operations to the public and to legal authorities.                          |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Anticipate technology law risks before they get out of control                                                        |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Implement practical steps to cope with technology law risk                                                            |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Better explain to executives what your organization should do to comply with information security and privacy law     |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Better evaluate technologies, such as digital signatures, to comply with the law and serve as evidence                |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Make better use of electronic contracting techniques to get the best terms and conditions                             |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |
| Exercise critical thinking to understand the practical implications of technology laws and industry standards         |          |         |                    |               |               |                               |                 |            |           |                  |              |               |               |               |               |