UNIVERSITY OF TARTU
Institute of Computer Science
Conversion to IT Curriculum

Mari Seeba

A Specification of Layer-Based Information Security Management System for the Issue Tracking System

Master Thesis (15 ECTS)

Supervisor: Prof Raimundas Matulevičius
Supervisor: Prof Ahto Buldas

Tartu 2019

A Specification of Layer-Based Information Security Management System for the Issue Tracking System

Abstract:

Organizations need to provide trust when entering into the new market, applying for new clients or partners or fulfill regulative requirements. ISO27001 standard and certification is the best known and the most adopted information security framework for verifying information security process compliance. Standard gives best practice guidelines to establish, implement, maintain and continuously improve the information security in the organization. Author has created the layer-based information security management system process, and proposes it to be integrated into issue tracking system. Thesis uses ISO27001 processes and goals analysis to derive layer-based ISMS tool specification for issue tracking platform. The specification is detailed on the level that is needed to validate the Jiras' ability to fulfill the specified requirements to get the organization in compliance with ISO27001 standard requirements. The results of this thesis may be used to develop an independent product for information security management on Jira platform.

Keywords:

Information security management, ISO27001, ISMS tool, compliance management, requirements engineering, layer-based ISMS

CERCS:

T120 System Engineering, computer technology

Infoturbe halduse tööriista spetsifikatsioon rakendamiseks töövoohalduse platvormil

Lühikokkuvõte:

Organisatsioonidele on oluline usalduse loomine, seda nii uute turgude ja klientide hõivamiseks kui ka regulatsioonide nõuete täitmiseks. ISO27001 standard on tuntuim ja kasutatuim infoturbe raamistik, mida sertifitseerimiseks ehk vastavuse kinnitamiseks kasutatakse. Standard pakub hea tava juhiseid organisatsiooni infoturbe halduse määratlemise, juurutamise, säilitamise ja parendamise läbiviimiseks. Siinse töö autor on loonud infoturbe halduse kihtsüsteemi protsessi ja teeb ettepaneku kasutada seda ISO27001 nõuete täitmiseks töövoohaldussüsteemi integreeritult. Töös analüüsitakse ISO27001 standardi protsesse ning eesmärke, et tuvastada infoturbe halduse kihtsüsteemi nõuded. Loodud spetsifikatsiooni abil on võimalik saavutada ISO27001 vastavus töövoohaldussüsteemi Jira abil. Töö tulemit saab kasutada eraldiseisva toote arendamiseks.

Võtmesõnad:

ISO27001, infoturbe haldus, vastavuse haldus, ISMS tööriist, nõuete tehnika, ISMS kihtsüsteem

Contents

1 Introduction

Whenever the information is handled, there are questions about information security – is data protected from unexpected changes, is data available for usage and only to authorized entities, who needs to see the data, and so on. Sometimes the data handling rules are detailed in contracts or stated by regulative acts. The other option is to have an information security management system (ISMS) compliance certificate.

ISMS certificate provides confidence for interested parties that the organization preserves the confidentiality, integrity, and availability of information by applying a risk management process and manages risks related to information adequately [9].

An internationally recognized and increasingly adopted information security standard for ISMS certifications is ISO27001[1] (International Standard ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements) [28].

The ISO27001 standard itself is altogether 22 pages, but implementation of the standard is complicated without specialized knowledge. General level clauses described in ISO27001 state that information security should be integrated with the organization's processes, it should be scalable, and it should be verifiably traceable by interested parties (i.e. the auditors). Based on this thesis author experience, there are several special tools to support organizations to get and maintain compliance with the ISO27001. The focus of these tools is to be compliant with ISO27001, not to manage the security as a natural part of the organization management process.

On the other hand, in most IT organizations, some workflow management system, like issue tracker or ticket management systems, are used. These tools give the verifiable traceability for internal processes. Issue management is integrated into projects and processes, and all members of the organization are using it (i.e. they know the principles of its usage).

Described situation motivated the thesis author to find a way to integrate ISMS management into issue tracking or workflow management tool. Background research revealed that there is no such kind of integrated solution on the market at the moment. For example, the Jira issue tracking system (developed by Atlassian) has a 40% market share of issue tracking systems [16]. Jira platform has more than 3000 extensions. However, Jira platform does not have an ISMS tool.

Several interviews with the target group revealed that the need for ISMS management functionality in Jira is desired and organizations would be ready to pay for the working solution if someone would implement this functionality [24].

[1] Here and after ISO 27001 standard is mentioned as "ISO27001" and no citation reference [9] is added

This thesis focuses on the proof of concept level the research questions (RQ):

1. How to manage an ISO27001 based information security management system using issue tracking tool, for example, Jira?
   (a) What are the ISO27001 processes of the layer-based ISMS tool to manage and trace?
   (b) What are the required issue tracking tool functionalities to implement layer-based ISMS tool?
   (c) How to systematize and visualize layer-based ISMS solution requirements?

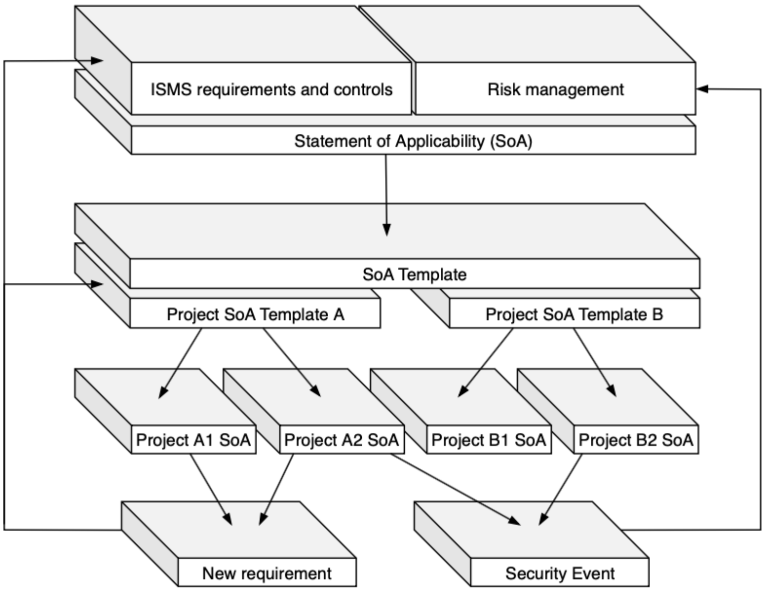


Figure 1. Layer-based information security management

The thesis provides the layer-based information security model and systematized layer-based ISMS model requirements to issue tracking tool features. Layer-based information security management model is a new approach to ISMS management. The main idea is to integrate information security requirements into processes and projects with the statement of applicability (SoA) layer (see Figure 1). Layer-based ISMS enables to bring information security requirement systematically into projects and processes, where an organization should implement ISMS. So it is possible to distribute the knowledge of information security over hole organization in required form implicitly. Statement of Applicability (SoA) is the central distribution artifact of layer-based ISMS. Every project and process can adapt itself to produce its SoA compliant to organization SoA. Any time the organization can monitor centrally the status of information security. Layer-based ISMS model integrates information security visibly into processes and projects. It is scalable and involves organization staff into ISMS in the most natural way. Layer-based information security model uses issue tracking tool features to generate templates of issues and import these templates to project issues.

This thesis consists of seven sections and three appendices.

Section 2 introduces the background of the ISO27001. Estonian Information System Baseline Security (ISKE) and ISKE tool creation story gives the background for thesis author and ISMS tool related problems. Section 3 describes motivation for this thesis by analyzing alternative options for ISMS management. ISO27001 standard outline, processes, and goals are analyzed in section 4. Layer-based ISMS tool processes and components are specified in section 5, using ISO27001 analysis results. Section 6 summarizes results of the interviews were conducted to validate specification.

Layer-based ISMS tool modeling methods and specifications are described in Appendix B and Appendix C. In appendices provided information is complete and self-contained for separate usage.

Thesis outcome systematization was inspired by: *Digital Business Analysis* by F. Milani [17] and *Requirements Analysis and Software Design* by L.A. Maciaszek [14].

Thesis is based on 13 years of experience in information security domain in role of consultant, auditor, implementer and coach. Authors previous work is related to developing Estonian national information security baseline system and tools. Author provides a novel idea on how to integrate information security management to projects and processes and proposes it to be integrated into issue tracking system.

2 Background

Section provides ISO standardization organization information and how the ISO27000 standard family was established. Estonian national information security baseline system history and current situation is providing background of the starting point of this thesis.

2.1 The International Organization for Standardization

The International Organization for Standardization (ISO.org) is an independent non-governmental international organization, which brings together experts from national standardization bodies and develops international standards [12].

ISO.org has developed a wide range of standards. In the ISO.org structure is ISO/IEC Joint Technical Committee 1 Sub Committee 27 (ISO/IEC JTC 1 SC 27), which is recognized to develop information security and privacy standards. Committee is consisting 78 members (49 participating members and 29 observing members. For example, Estonia is a observing member at the moment.) One of the scope topics of SC27 is the *"Management of information and ICT security; in particular information security management systems, security processes, and security controls and services."* [11]. The most known result of the SC27 work is standard ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. This standard is on the top of the most popular standards of ISO management system standards (based on the downloads counting[2]).

2.2 ISO/IEC 27001:2013 Information security management standard positioning

The motivation to publish the ISO27001 standard is explained by Edward Humpreys[7]. At the end of the 1990s when widely IT reached into every industry, the organizations understand the need for information security. Several technical standards were dealing with particular technologies. When the privacy issues arose and the need for information security knowledge of users directed to the new approach. Organizations began to search for non-technical standards that would address the business objectives for information security. One of these baseline controls were developed in Germany. IT Baseline Protection Manual was the origin of nowadays known BSI (Bundesamt für Sicherheit in der Informationstechnik) IT-Grundschutz. (An Estonian Three-level IT Baseline Security System ISKE bases on this German best practices [29].)

[2] `https://www.iso.org/popular-standards.html` Last access 15.05.2019

Humpreys [7] article tells that another significant example is the universal best/code of practice for information security (BS 7799) creation in 1992 by practitioners. This standard was well adopted in the UK and also in several countries outside the UK. This standard was submitted to ISO/IEC. On 2000 ISO adopted the standard to be ISO/IEC17799 "Information Technology - Code of practice for information security management." At 2005 there was the strategic decision to publish standard series about information security techniques under the name ISO2700X series. The second edition of ISO/IEC17799 was already named ISO27002. Starting the new series of standards, this opened the opportunity to develop the family of ISO2700x information security management standards. The flagship of the family is "ISO/IEC27001 Information technology — Security techniques — Information security management systems — Requirements" was published in 2005. It was adopted from BS7799-2. ISO27001 belongs to the family of management system standards that stand for continuous improvement philosophy (for example ISO9001 Quality management system standard, ISO14001 Environmental management system standard, ISO22301 Business continuity management system standard). The implementation of these management standards is similar and makes it possible for organizations to implement them simultaneously. When ISO.org published ISO27006 and ISO27007 (standard for accreditation of certification and auditing of ISMS), then it came possible to certify compliance to ISMS standard ISO27001.

Certifications of ISMS verifies the organizations' consistency to establish, implement, maintain and continuously improve the ISMS and through that it gives interested parties confidence that risks are adequately managed [9]. The ISO27001 does not give any restrictions on organizations structure or size, even not mentioning any technology. These principles give an opportunity, it can be adopted in small and also in large organizations in very different industry domains.

The main property of the ISO27001 is that it gives the framework of information security management in the organization. This universal approach is the reason why several countries have adopted their national standard on ISO27001 as a baseline. Several organizations develop other specific standards on that. For example, ENISA (the European Union Agency for Network and Information Security) is developing the privacy standards and admits that ISO27001 is the base to build the specific issue standards [3]. This is only one example of studies where ISO27001 arises to be as a base level standard for information security.

One of the databases about national cybersecurity management by the countries is the National Cyber Security Index (NCSI, developed by the e-Government Academy in Estonia [18]. This database contains among the other data links to national cybersecurity/information security standards or regulations to each country. This database can be helpful to find countries who use ISO27001 principles (see Sections 5.1 and 5.2 in the NCSI per country). This thesis author contributed to this NCSI methodology development as one of the experts.

In the scale of the world, there is more than 39 000 ISO27001 certified organizations all over the world and the number is growing each year quicker (positive change of ISO27001 certified organizations from 2016 to 2017 was 19%)[28]. In Estonia each year some organizations notify about the acquired ISMS certificate. In Estonia, one of the firsts software development companies owned ISO27001 compliance certificate was Cybernetica AS (2017). The thesis author participated in the process as an internal consultant of ISO27001 implementation.

2.3 Estonian ISMS and the need of tools

In Estonian public sector there is required to implement ISKE (Estonian information security baseline system). In nearest future the Estonian government needs to improve the information security management standard and plans explicitly to follow the ISO27001 direction. This also means that Estonian public sector needs ISO27001 compliant ISMS tool. This fact was one of the motivators to write this thesis. The Section will describe why Estonia did not choose the ISO27001 to be the national standard years ago and how they are approaching to the ISO27001 now. Short overview of the role of Estonian company Cybernetica AS[3] in this process is provided. Thesis author was Cybernetica employee for more than 13 years (2005-2019).

2.3.1 ISKE - Estonian information security baseline system

The long term Estonian representative of ISO/IEC JTC 1 SC 27 was Monika Oit (1952-2013), former head of information security department of Cybernetica and past president of ISACA Estonia chapter. She participated in 1999-2015 in ISO.org Joint Technical Committee ISO/IEC JTC 1 SC 27 as an official Estonian national representative during ISO17799 and ISO27001 first editions were published. She was also leading the consultation process for the Estonian government to find suitable national information security framework as a representative of Cybernetica.

Cybernetica conducted a study about national information security baseline system [4] for state owned information systems in 2003. The study was critical to ISO17799 because of its inconsistency of security objectives and granularity of the standard. Granularity was too low and required high qualification knowledge in the information security field from the implementer. In this time Estonian information security community was in its forming stage. It was too small to count that each local authority can find information security specialist with the required proficiency. The baseline was expected to be granular enough to understand and guide the

[3] https://cyber.ee

implementer without specialized knowledge in the information security field. The expected outcome of the study was the baseline security with its security measures catalog. The study [4] suggested to adopt the German IT Grundschutz Catalogs and to use it with the security classification guide. This classification guide [1] resulted in technical report compiled by Ahto Buldas, Monika Oit, and Valdo Praust, the researchers of Cybernetica team, in 1998. Also, the study suggested to develop the high-security level measures for the catalog based on Estonian local needs.

In 2003 Estonian Government published the first implementation guide of ISKE *(Infosüsteemide kolmeastmeline etalonturve)* and ISKE threat and security measures catalog[29]. Previously mentioned German BSI IT-Grundschutz was adapted to be the national baseline security standard of Estonia. The incentive to use the German baseline standard was explained by existing security measures catalog and free usage of this catalog.

The three-level baseline security assumes that organization can divide its information assets based on CIA (confidentiality, integrity, availability) requirements into security classes (high, medium, low) and spread the required security level to all system assets. This segregation of CIA security classes enables them to choose only needed level security measures from the catalog and optimize the process of risk management separately for each asset.

On the period of the first version implementation of ISKE, it was the proper solution, because it gave the needed security level just following the catalog measures. Implementer did not have to go through the full complex and time-consuming risk management process. Even when the implementer was not specialized in information security, catalog measures description said how to behave. This catalog was usable as information security textbook. The problem was that the catalog seemed to the users to be too complicated and frightened with its massive volume. The study [4] suggested to use hypertext format, but Information System Authority of Estonia (RIA) produced only PDF or ODT documents. The use of the ISKE catalogs in these formats was uncomfortable. (ISKE contained about 5000 pages of text. For comparison, the ISO27001 standard is only 22 pages. These comparison discussions did not take into account the fact that the objects under discussion were not in the same category - ISO27001 is implementation framework, ISKE is security measures catalog which also includes 20 pages of the implementation guide. ISO2700x series standards together are in a similar size with ISKE. However, representatives of implementer organizations did not apprehend the difference between the categories. Also, it was hard to explain the similarities and differences for needed effort for information security implementation in the case of ISO27001 and ISKE.

Later on, at the end of 2010th, the German BSI IT-Grundschutz confirmed the compliance to ISO27001. That confirmation did not automatically transfer to confirm the compliance of Estonian ISKE. ISKE was not directly translated from German; it was adapted by adding Estonian specific modules, high-security level measures and local implementation and auditing guidelines. RIA (responsible institution for maintaining ISKE) published the mapping tables between ISKE and ISO/IEC27001:2005, but compliance was not officially approved. Thesis author compiled ISKE and ISO27001:2013 mapping for internal use of Cybernetica projects [23]. This mapping made clear that there is full compliance in security measures, but the management of ISKE misses distinct management processes. The primary purpose of the mapping was to show that ISO27001 is a framework and gives only the directions. In the same time, ISKE gave precise controls to implement. Also, the implementation guide of ISKE provides the detailed establishing and implementation steps, but maintenance and continual improvement are covered briefly[8]. It is possible to say that if to use the ISKE catalogs for the ISO27001 the implementatin, then the system will be compliant to both standards. ISKE alone could not reach to the compliance with ISO27001.

2.3.2 The tools for supporting the implementation of ISKE

RIA supported state organizations implementation of ISKE with document templates and pilot project deliverables, also with developing the unique ISKE implementation tool (ISMS tool for ISKE). The first analysis of this tool was made in 2007 by Tepinfo OÜ [27]. At the time there were no best practices and the understanding of how to manage information security in an organization. It was also complicated to explain the need for information security to people outside the ICT domain. The organizations did not have established the role of information security officer/specialist. The target group of the tool was in the formation.

Smartlink OÜ made the second iteration of analysis [26] and delivered the ISKE tool in 2010. The thesis author participated as ISMS expert and adviser in the preliminary phase of the development project to give the vision, vocabulary and the understanding of information security management to developers. ISKE tool was implemented and used by organizations, but the background situation changed too quickly, and the tool did not satisfy the users. At same period IT departments of public sector organizations and security officers were centralized to separate service providing institutions. The need changed, how to get an overview of related institutions information security. The ISMS tool was inflexible, and the **scalability** was a problem. ISKE was developed as a **tool for one person**. It was complicated and not **integrated into organizational processes**. The primary tool purpose was to trace the compliance to ISKE in relation with assets. Also, the ISKE catalog was not adequately formatted and was therefore impossible to use it in automated manner. The tool was usable only with the ISKE textbook with its more than its 5000 pages.

In 2014 thesis author participated in the analysis of ISKE tool refinement suggestions project as the project manager and adviser (participated in interviews and solution discussion) in the Cybernetica AS [25]. After that, the procurement for development of suggested refinements of the ISKE tool was unsuccessful. However, the positive result of this ISMS tool for ISKE refinement analysis was the suggestion to format ISKE text to be readable to the machine and manage it in wiki-based ISKE Portal and to cease to use ISKE catalog in PDF and ODT-format. In 2015 Cybernetica AS team developed this ISKE portal. The thesis author was the project manager, domain expert (giving input to the analyst), validation and verification tester and technical writer in this project. For the result of this project, there is formatted, searchable and manageable machine readable ISKE catalogs text in ISKE portal [10].

During the 2018 German BSI finalized the transition to a new approach of the baseline security and named it IT-Grundschutz-Kompendium [13]. On that, the Estonian government has reacted with procurement to develop Estonian information security standard for the end of 2020[4]. The standard should be based on the German solution but not only translated. There is a need for a full ecosystem of establishing, implementing, maintaining and improving the national standard, supportive training, materials, and implementation tool. The standard should direct the users explicitly to be compliant with ISO27001. The author of the thesis supported RIA with ideas for mentioned procurement.

The organizations adopting Estonian National Information Security Standard need toolset to support the information security management process. Based on interview results, government institutions, participated in the interviews, are using Jira for their workflow management and they are interested of the possibility to use same platform for ISMS implementation also. If possible, they prefer Jira instead of any separate unique tool [24].

The Estonian National Information Security Standard is an example of ISO27001 usage as a framework for information security management systems, which needs supportive ISMS tool.

2.4 Summary

ISO27001 is related to number of information security management practices. For example, Estonian ISKE framework does not recognize ISO27001 management. There is active movement to use international standard to complement existing

[4] https://www.ria.ee/et/ametist/riigihanked-ja-hanketeated.html Last access 13.04.2019

information security management. Information security standards are containing lots of details there are no well suited tools for everyday usage, because tools are following security standard flows and not organization organic processes.

3 Motivation

The ISO27001 does not make advisement or restrictions on tools to manage ISMS. Organizations are free to choose method and/or tool for purpose. This Section compares different tools used and provides justification to use issue tracking tool for ISMS management.

3.1 Comparision of ISMS tools

When organization decides to implement ISMS, it starts to look for and compare suitable tools. It is possible to distinguish six different kind of tools. These options can be used separately or simultaneously or in part. The most straightforward option for the tool is any spreadsheet program (for example, Microsoft Office Excel, Libre Office Calc). Managing ISMS in a spreadsheet means that implementor needs to start implementation from scratch and requires a lot of knowledge and experience.

Possibility to simplify this spreadsheet solution is to buy ISMS implementation templates set for spreadsheet program. There are several providers of predefined templates for (usually) Microsoft Office products on the market[5].

The organization can outsource the consultant service to help the implementation of ISO27001. Then the organization needs good motivation to maintain result and keep information security processes running without consultant involvement.

The organization can buy license of a purpose built ISMS tool. It covers requirements of the ISO27001 standard, but these tools are complicated standalone tools limited with one user only. Sometimes these tools have interfaces to integrate them into existing systems, but it is complicated and expensive because it needs special development and continuous integration.

Workflow management solution used by organization can be used also for ISMS management. For example, any issue tracking tool with the internal wiki. Members of the organization know how to use the tool; they are familiar with tool features and workflows. If to make an assumption, that this kind of tool has ISMS management functionality, then it is possible to compare workflow management solution with previously mentioned options.

Table 1 gives an comparison overview of tool properties assessed on the scale 1 to 5. The best option gets 5 and the weakest 1 point. The presented sequence is based on the thesis author experience observations and interviews from the last ten years.

Table 1 characterizes different tool properties based on this thesis scope:

[5] For example, https://www.iso27001security.com, https://certikit.com/ Last access 15.05.2019

Table 1. ISMS tool comparing

	Learning Curve	Integration	Scalability	Traceability	Group work	Cost	**Total**
Speardsheet	5	1	1	1	1	1	10
Template set	2	3	2	3	4	2	16
Consultant	3	4	3	2	3	5	20
Compliance tool	1	2	5	5	2	4	19
Workflow management tool	4	5	5	4	5	3	26

Learning curve - characterizes how complex the tool is for users and how quickly users can get used with the tool features. The best solution is with the shortest learning curve.

Integration - tool integration into the projects and organizational processes to follow ISMS principles. The best solution is the most easily integrateable solution.

Scalability - ability to follow the organization changes driven by business needs. The best solution is able to integrate ISMS into new project or processes without overhead.

Traceability - evidence traceability of the activity sequence for example, process - asset - risk - measure - verification. The best solution visualizes the journey for example from risk and control to asset, measure, verification of the measure, improvement.

Group work - characterizes the tool usage - how many users are working with the same tool in the same time to manage security events and risks. The best solution involves all process and project participants

Cost - investment estimation for the organization of the ISMS tool. The best solution is with lowest price.

Total - summarizes the ranking of the tool properties. The best is with the highest score.

The best tool by the Learning curve is *spreadsheet.* The worst one is a new *compliance tool* for ISMS. The reason is, that compliance tool follows the ISO27001 logic, but not the existing everyday workflow of the organization processes. It is hard to study, understand and adapt to the organization. **The best by integra-**

tion into processes is the *workflow management tool*, what organization members already use for workflow tracing and what they have already implemented into their processes. The best tools by scalability are both the *special tool* and the *workflow management tool*. Usually, *compliance tools* are designed to fit in every organization. For traceability the best tool is the *compliance tool* and the *workflow management tool*, issue trackers give enough traceability. The Group work becomes an issue when there is a need to maintain the ISMS tool and share the tool functionality with organization members. The score of Group work is higher for *workflow management tool* because organization members use it as a group working environment for everyday workflow. Cost for the *compliance tool* is high, and the organization usually does not invest into the tool to buy it for everyone. For *workflow management tool,* it is more probable that the organization invests into some plugins and user licenses because the organization knows and uses the tool already. Organizations are ready to pay a higher price for the trusted tool. Tool prices vary largely. The lowest price is for *spreadsheet.*

The ISMS tool property comparing analysis shows that organizations should use the *workflow management tool* for successful ISMS management because of the optimal time to learn to use it, the possibility to integrate it into projects and the high score for Group work functionality and the optimal price. The aspect to follow is that the workflow management tool should provide the functionality to support in Section 4 listed ISMS processes.

3.2 Jira for ISMS management

Jira platform developed by Atlassian is chosen as an example of a workflow management tool for this thesis.

Jira is a most popular tool (40% of market share)[24] for software developers because it has managed to go with time - it supports agile workflow features (Kanban, Scrum or basic project management functionality of software development). Jira is developed as an object-oriented solution. Jira provides to the users the issue management with its workflow defining possibilities and history view (traceability), custom fields and issue linking between projects and issues relationship features; projects may have their issues from imported CSV file, Board views are for reporting and tracing. The mentioned features are essential to fulfill ISMS management tool component requirements specified in Section 5.6.

Jira has a lot of third-party add-on solutions (more than 3000) and proper documentation for configuration. At the moment Jira marketplace does not include any add-ons for ISO27001 compliance. However, Jira has risk management compliance tool (add-on solution). Jira has tools for document management and asset management, which are mandatory for ISMS.

For risk management organization can use SoftComply Risk Manager[6]

From Atlassian Marketplace. Risk management add-on is already proved itself to be compliant with regulatory requirements for a safety standard. However, the risk management process described is compliant with ISO27001 requirements also.

For asset management in Atlassian Marketplace there are provided several options. For example, Riada Insight[7] can be used.

For document management organizations using Jira also using product named Confluence[8] developed by the Atlassian.

The modeling of the ISMS processes for this thesis used the mentioned risk management tool functionality.

Thesis author contacted with RiskManagement tool developers from SoftComply and tested some functionality in their Jira test environment.

3.3 Summary

Comparing different ISMS tools using criteria defined by author, revealed that integration with workflow management (issue tracking tool) is best matching solution for ISMS management. Author chose issue tracking tool Jira which provides necessary features to be used for implementing layer-based ISMS. There are no existing ISMS solutions for Jira. This is the motivation to analyze and develop specification for such tool.

[6] `https://marketplace.atlassian.com/apps/1216361/softcomply-risk-manager` Last access: 10.03.2019

[7] `https://marketplace.atlassian.com/apps/1212137/insight-asset-management` Last access: 10.03.2019

[8] `https://www.atlassian.com/software/confluence` Last access: 10.03.2019

4 ISO27001 structure and text analysis

ISO27001 objectives analysis is required for ISMS tool specification. Section covers standard structure introduction. Analyze includes necessary ISMS business processes and goals for layer-based approach.

4.1 ISO27001 structure

ISO27001 [9] is built up as a management system standard. Common terminology is defined in ISO27000 for standards in the family. When an organization claims to certification to verify the compliance to ISO27001 standard requirements then the clauses 4 to 10 of ISO27001 are mandatory, normative ISO27001 Annex A security objectives should be justified if an organization decides them to be non-applicable.

The standard clause 4 requires the organization to understand the context, interested parties, and issues that influence organization business objectives. Clause 5 defines the leadership commitment issues and information security policy context. Clause 6 directs through the risk management concerning security objectives planning and risk treatment plan. Clause 7 deals with supportive issues - resources, competence, awareness, communication, and documented information. Clause 8 gives directions to perform operations which were planned in Clause 6 when implementing the risk treatment plan. Clause 9 gives the instructions to performance evaluation methods like monitoring, measurement, internal audit, and management review. Clause 10 requires continuous improvement of information security management system. ISO27001 Annex A is divided into 18 control objectives and then into 114 controls.

Each organization implementing the ISO27001 should produce and maintain the document named Statement of Applicability (SoA). This document should contain information about ISO270001 Annex A controls - which of them apply to the organization and which are not (with justification) and provide details when, why and by whom the SoA was updated and approved.

The standard is developed by practitioners - that reflect from the defined processes and their regularity or sequence, which makes the standard understandable to users. But standard itself is hard to read, because every sentence and word carries the meaning of requirement.

4.2 ISO27001 goals for ISMS

The ISO27001[9] goals for ISMS can be summarized as follows:

(a) the ISO27001 gives the requirements for establishing, implementing, maintaining and continually improving of information security management.

(b) The adoption of the standard should be the strategic decision of the organization.

(c) The purpose of the ISMS should be to give the confidence to interested parties that the risks are managed.

(d) ISMS should be integrated into all parts of the organization and processes.

(e) ISMS should be scalable in accordance with organization needs.

(f) Standard requires to relate all information security requirements to business needs.

That makes up the reasonable task for the ISMS tool.

4.3 Identified processes

Author conducted thorough text analysis on ISO27001 standard text to identify the ISMS business processes. These processes must be supported by proposed layer-based ISMS solution.

ISO27001 requirements can be fulfilled using eight processes: (1) Define information security policy; (2) Compile Statement of Applicability; (3) Define Subpolicies ; (4) Security event management (includes incident management); (5) Project or process management; (6) Internal audit; (7) Management review; (8) Risk management (integrated into every process mentioned).

These processes cover standard clauses and include risk management as a natural part of each process. The controls from ISO27001 Annex A can require internal self-defined processes.

4.4 Summary

The thesis uses mentioned ISO27001 context goals and processes for modeling baseline of the layer-based ISMS.

5 Specification of the layer-based ISMS

The Background Section 2 described the origin and usage of ISO27001 standard and the reasons why it is so widely used, also were mentioned the problems arised with ISMS tool development. Section 3 illustrated why should organizations choose the workflow management (issue tracking) tool to be an ISMS tool platform. This Section describes steps used to analyze ISMS requirements for Jira issue tracking tool. Analyze includes ISMS management process workflow to be used with ISMS tool.

5.1 Scope

The scope of the study focuses on specifying the ISO27001 requirements from its clauses 4 to 10. The standard ISO27001 Annex A is taken into account on the aggregated level. Every organization designs its specific security objectives and measures given in each control of ISO27001 Annex A.

This thesis does not cover following ISMS components: risk management, asset management, and document management. These components are existing add-ons of Jira and can be used to implement full-scale ISMS.

Jira core functionality is used to implement ISMS tool functionality. Focus is to understand which functionality from the Jira is required for ISMS. The context interfaces related with ISMS tool are illustrated on Figure 2.

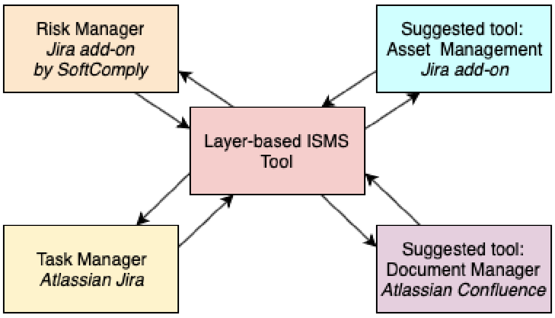


Figure 2. Related products of ISMS tool.

ISMS tool is positioned in the center of the Figure 2. On this thesis view, surrounding parts are mandatory for ISMS adoption. This study does not consider integration requirements of these products. It is assumed that these products are possible to integrate through linking the relevant object to the ISMS project issues. In the specification there is explicitly shown the linkage to Risk Management tool.

5.2 Steps of the study

This Section outlines the steps taken to specify layer-based ISMS process and develop the ISMS tool requirements for issue tracking tool functionality. Overview of the steps of the study is given in Table 2. Table consists information about the step, its input, expected output, tools used to compile result and section references of the detailed description and the work result in this thesis.

Table 2. Steps of the study

No.	**Name of the step**	**Input**	**Expected output**	**Used tools**	**Section**
1	ISMS tool goal analysis	ISO27001 text (see Sec. 4.2)	ISMS tool goals, specification to research question (RQ) (a)	i* modeling language[5], PiStar[19],(see Sec. B.1)	5.3, C.2
2	ISMS process analysis	ISO27001 text (see Sec. 4.3) and output of step 1; SoftComply Risk Manager tool principles [21]	ISMS management business processes, specification to RQ (a)	BPMN, Signavio, (see Sec. B.2)	5.4, C.4
3	ISMS tool functionality	Output of step 2 (ISMS tool pool)	ISMS tool use case diagram, specification to RQ (b)	UML[22], Signavio, (see Sec. B.3)	5.5, C.5
4	ISMS tool functions	Output of step 1, 2 (ISMS tool pool) and 3	Use case descriptions for ISMS tool, specification to RQ (b)	Use case template [20], (see Sec. B.3)	5.5.1, C.6
5	ISMS tool components	Output of step 4	ISMS tool components class diagram, specification to RQ (c)	UML[2], Signavio, (see Sec. B.5)	5.6, C.7
6	ISMS tool specification validation	Output of steps 1, 2 and 5	specification to research questions	Interviews, completeness analysis	6

Following sections provide examples and reasoning for each step of the Table 2. Appendix C contains full self-contained specification of layer-based ISMS tool.

5.3 ISMS tool goal analysis

This thesis goal modeling is made at high level to show the product and organization strategy relation to ISO27001. ISO27001 standard defines the goals for the organization ISMS (see Section 4.2). Goals can be listed as follows [9]:

G0 ISMS gives confidence to interested parties that the organization manages the risks adequately – interested party can trust the organization who can prove that ISO27001 requirements are adapted

G0-1 ISMS implementation is strategic decision – the top management is interested in the successful ISMS implementation and gives his commitment to that

G0-2 ISMS is based on ISO27001 requirements

G0-3 ISMS is assessable –compliance assessment to ISO27001

G0-4 ISMS is part of and integrated with the organization's processes and overall management performance – processes under the scope of ISMS are adapted to use information security rules, but also the opposite way - ISMS should be implemented into the existing procedures and processes

G0-5 ISMS is established – organization knows its information security requirements and context, risk assessment is done, procedures are designed

G0-6 ISMS is implemented – information security policies and processes are communicated and functioning

G0-7 ISMS is maintained – information security policies and processes performance is monitored and measured

G0-8 ISMS is continually improved – information security policies and processes functioning monitoring and measuring results are evaluated and refined based on risk assessment

G0-9 ISMS is scalable following the needs of the organization – the organization can change its processes, organization structure, grow or decrease but still is able to take into account information security requirements in defined level based on risk criteria

G0-10 ISMS is a part of management system – information security is supporting business objectives and taken info account when planning business objectives

G0-11 ISMS is verifiably managed – there are documented evidence of information security management performance

On the figures there are actors mentioned in the ISO27001 standard clauses 4 to 10: (i) **Organization** itself as an entity (the organization as Actor decomposition is managed on business process modeling (see Section C.4)), (ii) **Interested party** (any external entity whose interest is that the organization manages his information security adequately), (iii) **Management**, (iv) **ISO.org** who provides the ISO27001 standard and its requirements and (v) **Auditor** who can be internal or external auditor in this context.

Goal modeling i* (i-star) modeling language [5] was used to reason *who?* and *why?* needs the ISMS tool.

Figure 3 illustrates who are the Actors (interested parties) of the ISMS implementations and what are their interests. Organization internal goals to be achieved are shown separately. This model visualizes *who* and *why* they participate in the scope of ISMS of organization.

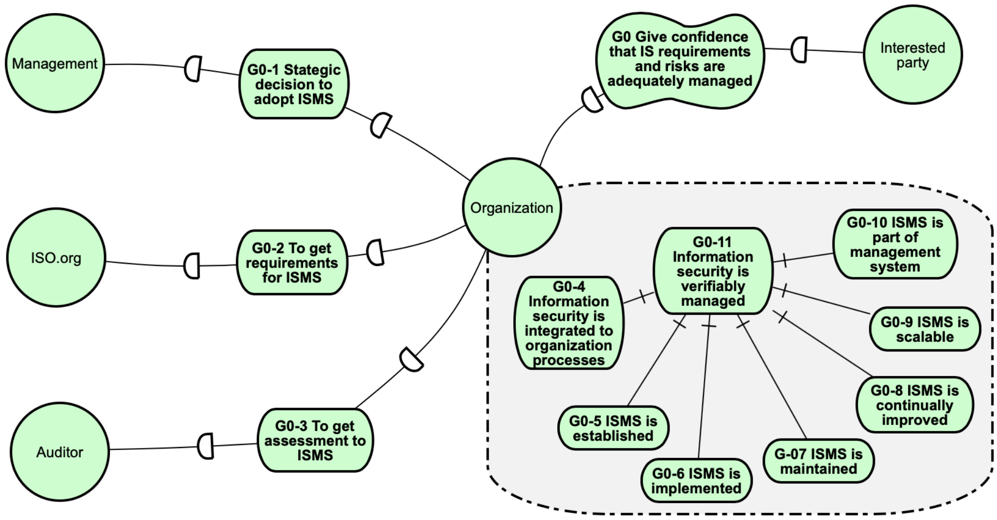

Management
G0-1 Stategic decision to adopt ISMS
G0 Give confidence that IS requirements and risks are adequately managed
Interested party
Organization
ISO.org
G0-2 To get requirements for ISMS
G0-11 Information security is verifiably managed
G0-10 ISMS is part of management system
G0-4 Information security is integrated to organization processes
G0-9 ISMS is scalable
G0-8 ISMS is continually improved
Auditor
G0-3 To get assessment to ISMS
G0-5 ISMS is established
G0-6 ISMS is implemented
G-07 ISMS is maintained

Figure 3. G0 ISMS goals.

The second Figure 4 illustrates the ISMS tool goal dependencies focusing on organization with the same Actors of detailed specification Figure 3. On the Figure 4 there is added an Actor – the ISMS tool, the focus point of this specification. The figure shows which goals should be managed with ISMS tool (colored in violet). These goals are G0-2, G0-4, G0-9, G0-10, G0-11. Special attention is on the direction of the goals - ISMS tool needs the requirements to be defined by organization (G0-2). The ISMS tool quality depends on that. Goals G0-5, G0-6, G0-7 can be melted into other goals as gathering the evidence of ISMS performance. The processes itself should be done by organization.

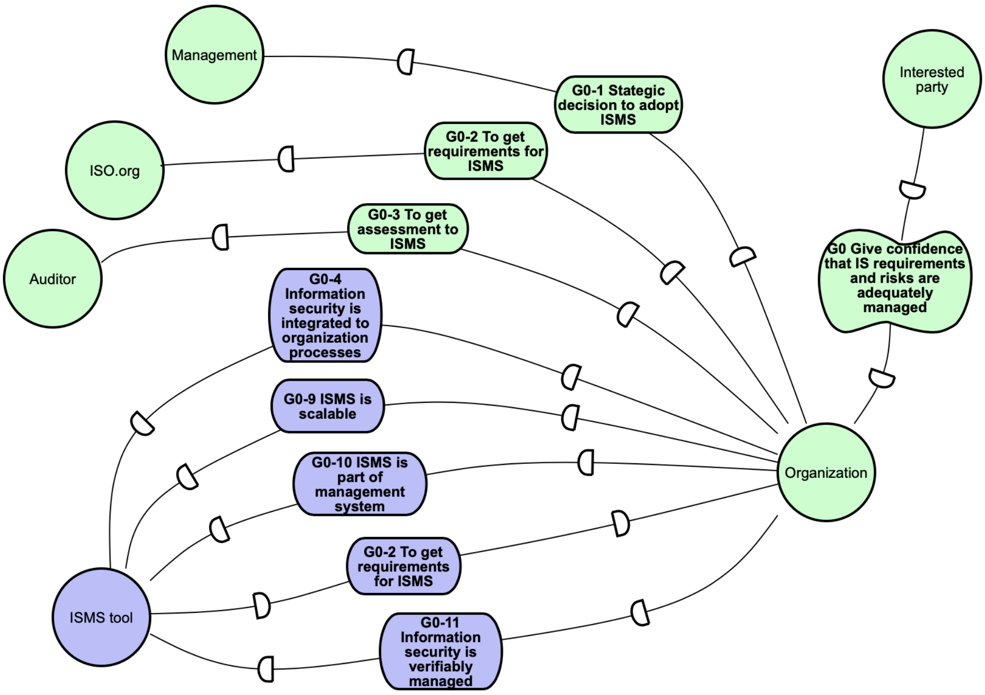

Management
ISO.org
Auditor
Interested party
G0-1 Stategic decision to adopt ISMS
G0-2 To get requirements for ISMS
G0-3 To get assessment to ISMS
G0 Give confidence that IS requirements and risks are adequately managed
G0-4 Information security is integrated to organization processes
G0-9 ISMS is scalable
G0-10 ISMS is part of management system
G0-2 To get requirements for ISMS
G0-11 Information security is verifiably managed
Organization
ISMS tool

Figure 4. ISMS tool goals.

Each goal has its unique ID-s (starting with "G") which are shown on figures and also mentioned in specification textual part in ISMS tool functions descriptions (see Section C.6).

The goal model is based on ISO27001 textual analysis. The goal modeling gave the direction, which kind of functionality should be realized with ISMS tool features to archive these goals.

ISMS tool goals can be concluded that ISMS tool main purpose is to help scalably integarate ISMS into all organization processes and trace activities to get evidence as a natural part of organization management system.

5.4 ISMS process analysis

Section describes ISMS processes based on text analyze of ISO27001 standard (Section 4.3) using layer-based ISMS approach.

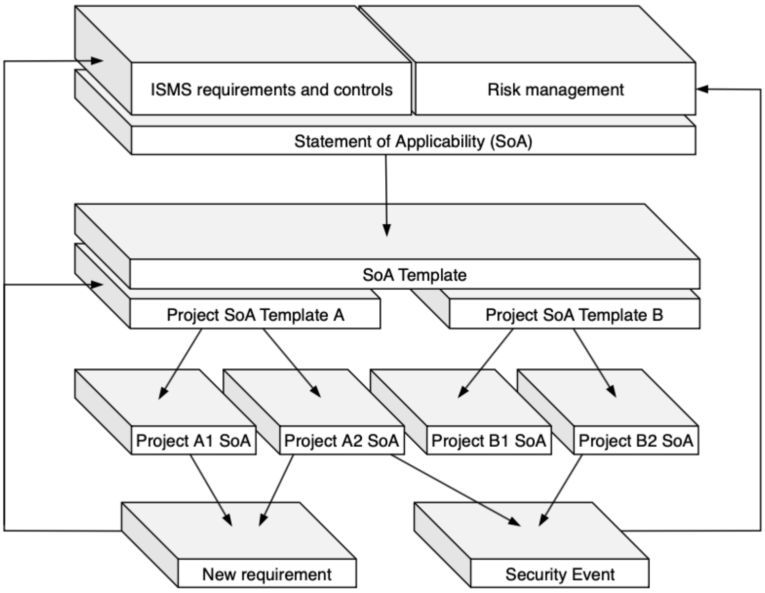


Figure 5. Layer-based information security management

5.4.1 Description of the layer-based ISMS tool concept

Figure 5 illustrates the layer-based information security management solution concept, which should be supported by processes. Information security requirements and controls together with risk management direct the organization statement of applicability (SoA). SoA contains the principles how ISMS should be implemented. These principles need to be spread to all organization projects/processes. The layer-based information security enables to use the same SoA template to adopt it for each project/process. The feedback system works through the security events or new and changed requirements as an input to risk management and organization context analysis.

Each process and/or project can adapt and track SoA issues with adding specific details or excluding some non-applicable issues. Central ISMS project gathers evidence of security requirements implementation in processes and projects through reports and board functionality.

5.4.2 Business processes modeling for ISMS tool

For organization compliance with ISO27001 requirements, standard does not accept any exclusions from the Clauses 4 to 10 [9]. General model of business processes of ISMS are on Figure 6. There are defined eight sub-processes.

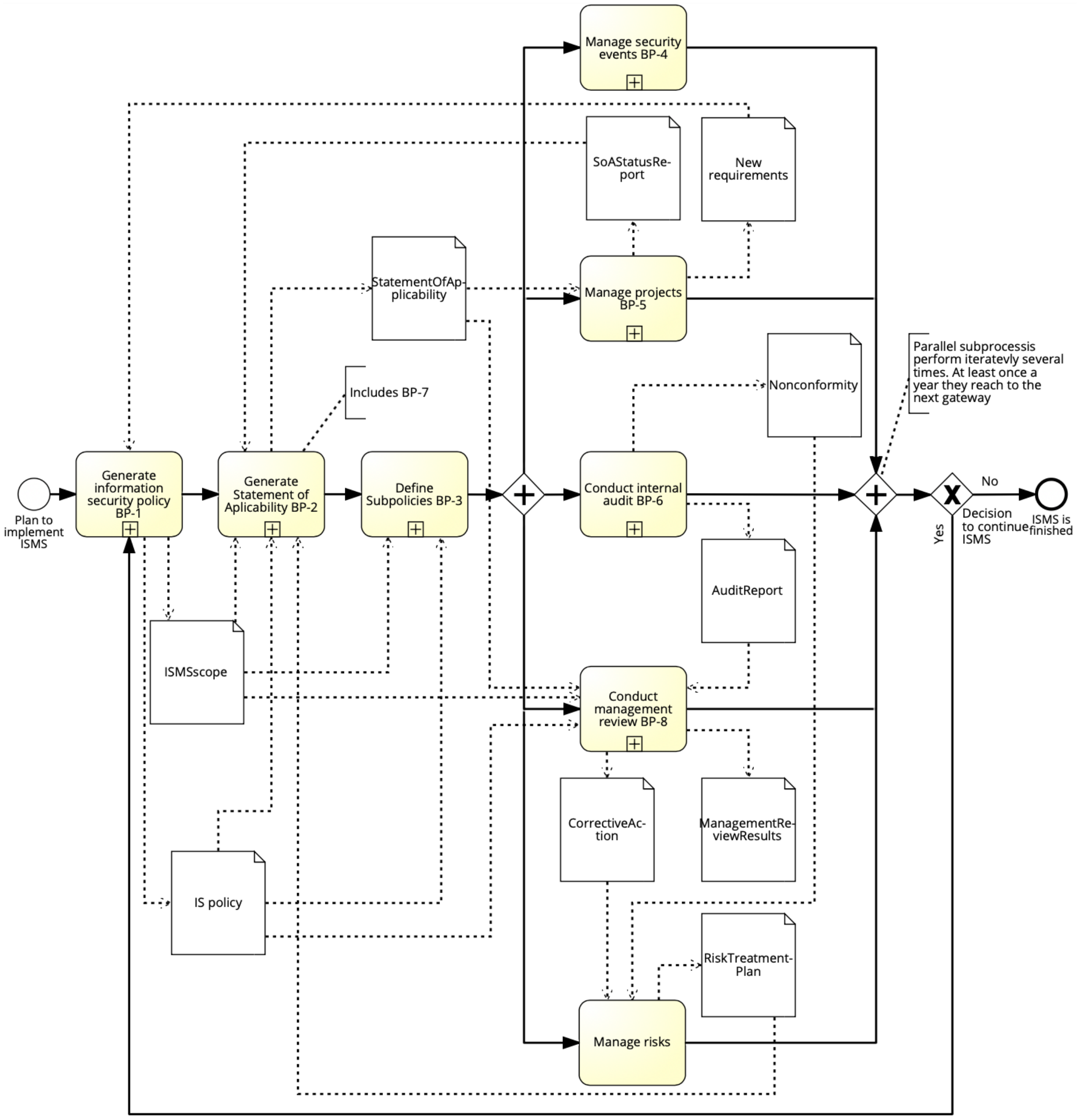

Manage security events BP-4
SoAStatusReport
New requirements
StatementOfAplicability
Manage projects BP-5
Includes BP-7
Nonconformity
Parallel subprocessis perform iteratevly several times. At least once a year they reach to the next gateway
Plan to implement ISMS
Generate information security policy BP-1
Generate Statement of Aplicability BP-2
Define Subpolicies BP-3
Conduct internal audit BP-6
No
Yes
Decision to continue ISMS
ISMS is finished
AuditReport
ISMSscope
Conduct management review BP-8
CorrectiveAction
ManagementReviewResults
IS policy
RiskTreatmentPlan
Manage risks

Figure 6. BP-G ISMS general business model.

They are chosen by the principle, that they cover standard mandatory clauses. Additionally is given the general process/project management model for controls implementation of ISO27001 Annex A. These eight processes were mentioned in Section 4.3. The detailing level of the represented business process models is chosen by the need for ISO27001 text and human activity tasks. Each organization can add to the models its specific stakeholders or detail actions by their own needs. The process of composing the models was divided into two phases: at first, was modeled the human activities what satisfied the ISO27001 requirements and goals; in the second phase were added ISMS tool specific activities into a separate pool. Then were added message flows between Organization and tool activities.

The processes follow the logical sequence of actions: establish, implement, maintain and improve. The processes are iterative in some parts or entirely to characterize the cyclicalness of ISMS. For input of the business process analysis is used the ISO27001 text and the thesis author domain expertise to investigate the processes to be compliant with ISO27001 requirements. Figure 6 gives the understanding of the sub-processes relationship to each other and the sequence. Parallel sub-processes could perform iteratively several times a year. As the process is continuous, the output documents are inputs for another process in the next iteration. Input and the starting trigger for that general process is the strategic decision to implement ISMS in the organization (G0-1). The output of the process are documented evidence (G0-11) that can give the auditability of ISMS establishment (G0-5), implementation (G0-6), maintenance (G0-7), and improvement(G0-8) of ISMS performance. The process ends on the case the management decides not to continue with ISMS.

Another example is adapted project management process (see Figure 7). Internal processes may use the project management process by adding their details. The project management model is basing on the project management workflow model suggested by recognized textbook [6]. Figure 7 shows project management process activities with blue background. ISMS activities are added with yellow background. The starting point of the process is the new project creation. The Actor of the process is Project Manager. To keep the model simple, it does not show the other project members activities implicitly. The input to the project is SoA template or already adapted project SoA template that gives links to relevant documents and requirements of ISMS (G0-2, G0-4). Process has a collapsed subprocess, which is expanded on Figure 8). Subprocess is executed for each issue, which is security related issue and should be linked to SoA project. The outputs of the project management are security event reports (if relevant) and evidence of followed process (entry log/history in the ISMS tool) (G0-11, G0-4, G0-9, (G0-5, G0-6, G0-7, G0-8)).

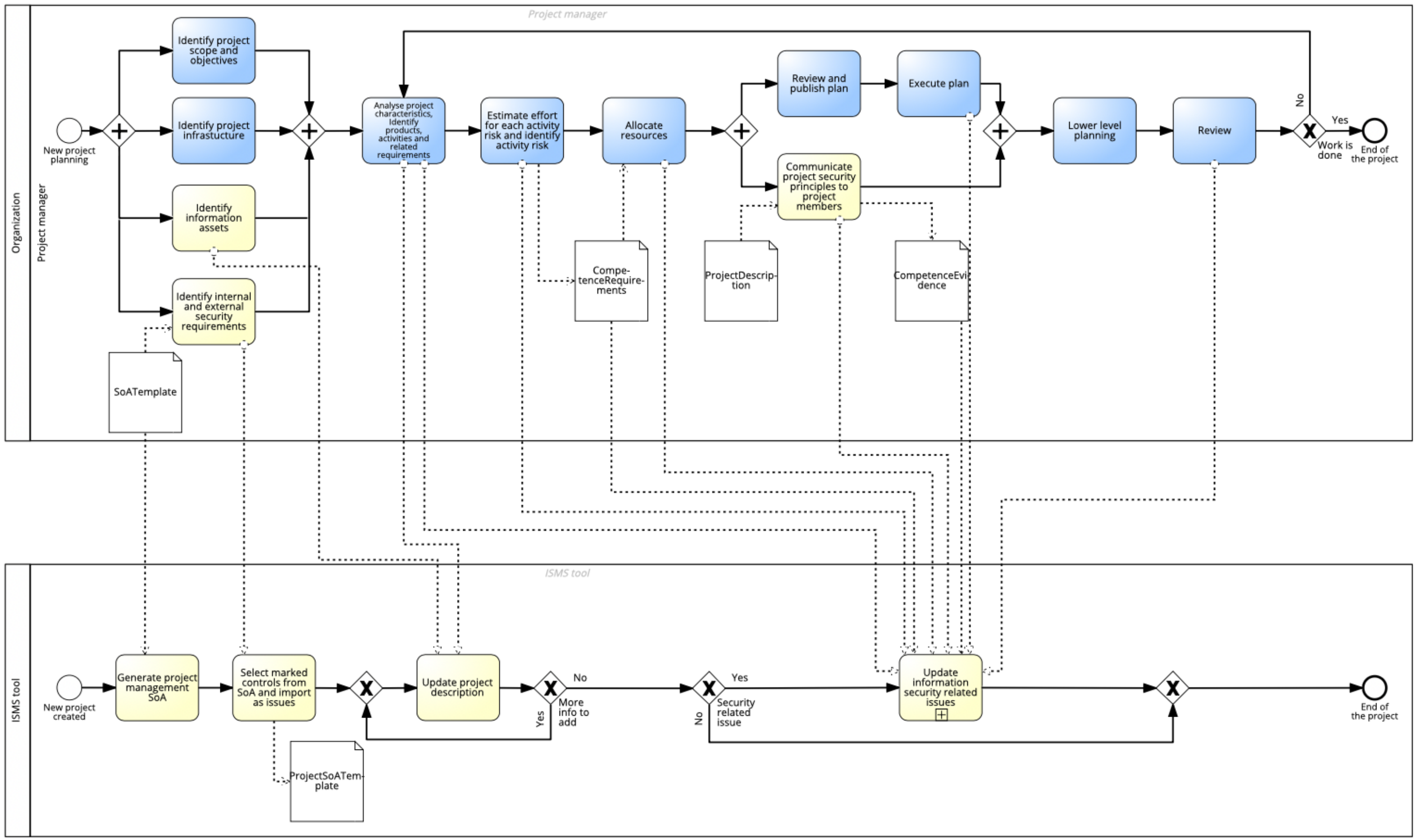

Organization
Project manager
Project manager
New project planning
Identify project scope and objectives
Identify project infrastucture
Identify information assets
Identify internal and external security requirements
SoATemplate
Analyse project characteristics, Identify products, activities and related requirements
Estimate effort for each activity risk and identify activity risk
Allocate resources
Compe-tenceRequire-ments
Review and publish plan
Execute plan
Communicate project security principles to project members
ProjectDescrip-tion
CompetenceEvi-dence
Lower level planning
Review
No
Yes
Work is done
End of the project
ISMS tool
ISMS tool
New project created
Generate project management SoA
Select marked controls from SoA and import as issues
ProjectSoATem-plate
Update project description
No
Yes
More info to add
Yes
No
Security related issue
Update information security related issues
End of the project

Figure 7. BP-5 Project management (adapted from [6]

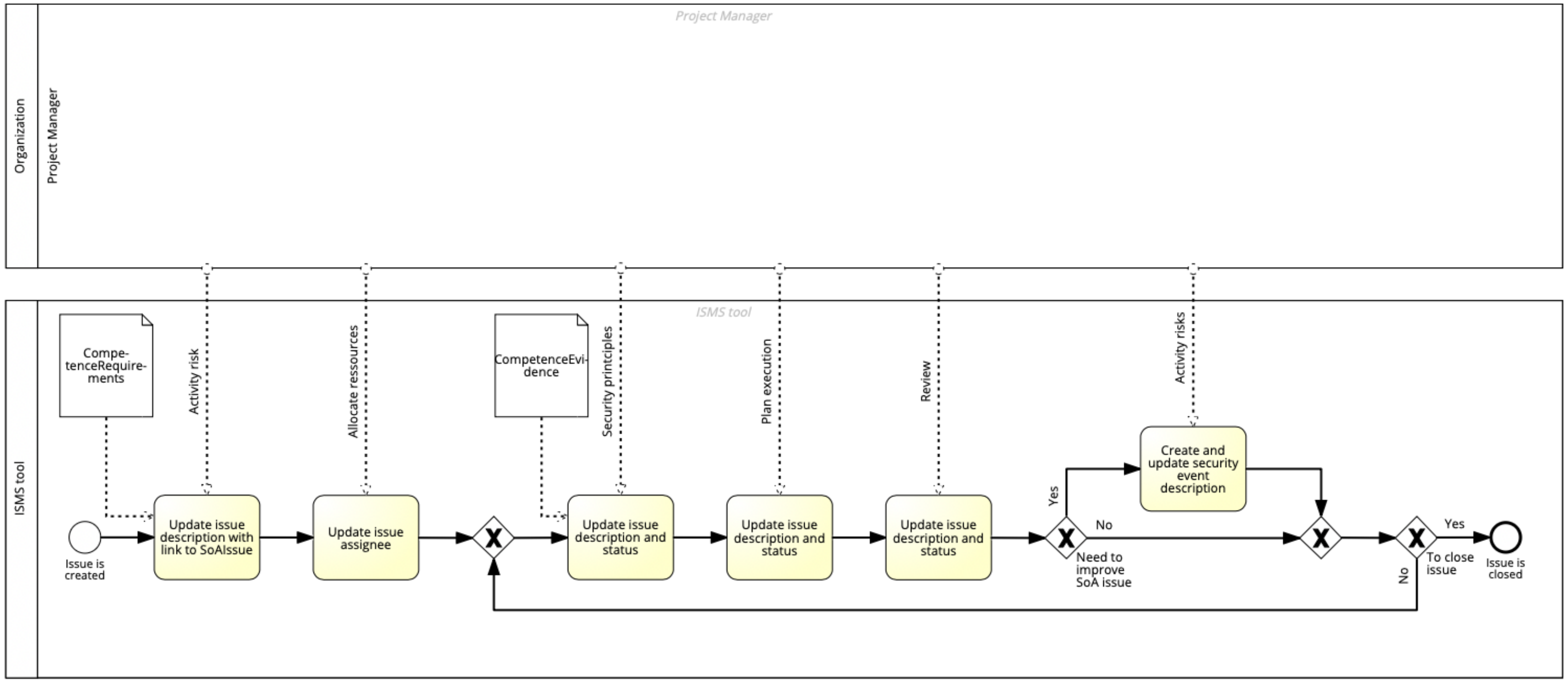
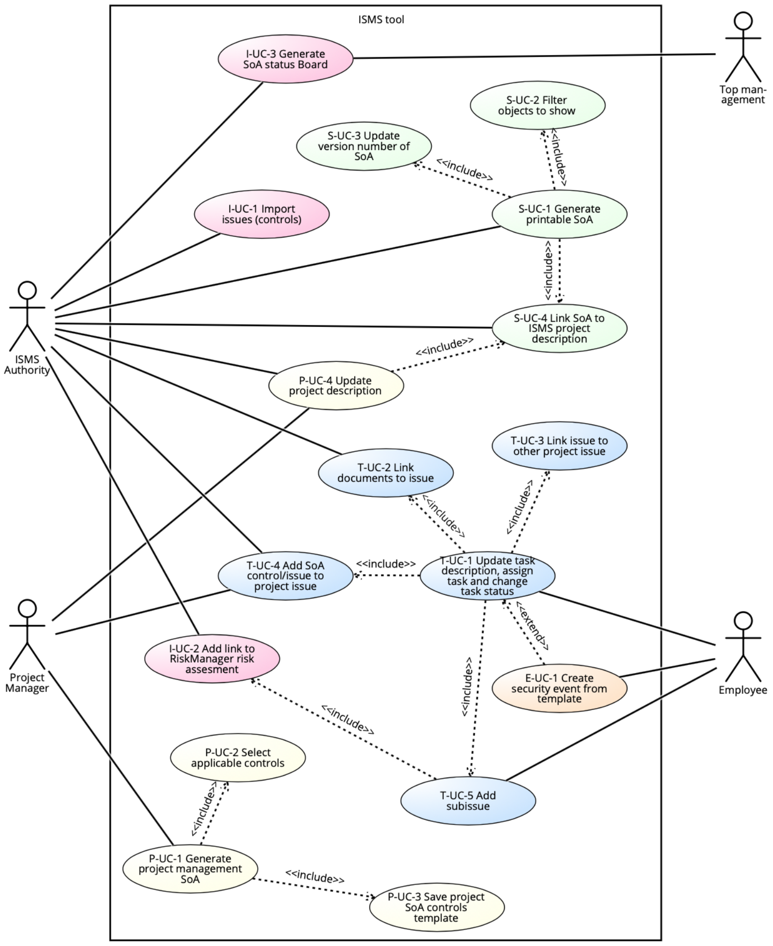


Figure 8. BP-5a Project management subprocess: Update information security related issues

5.5 ISMS tool functionality

Based on the business process analysis (see Section C.4), each modeled activity in the ISMS tool pool was analyzed separately to find similarities and the need to have the use case(s). The result was ISMS tool use case diagram that shows the needed system functionality of ISMS tool (see Figure 9).



ISMS tool
I-UC-3 Generate SoA status Board
Top man-agement
S-UC-2 Filter objects to show
S-UC-3 Update version number of SoA
<<include>>
<<include>>
I-UC-1 Import issues (controls)
S-UC-1 Generate printable SoA
<<include>>
S-UC-4 Link SoA to ISMS project description
ISMS Authority
<<include>>
P-UC-4 Update project description
T-UC-3 Link issue to other project issue
T-UC-2 Link documents to issue
<<include>>
<<include>>
T-UC-4 Add SoA control/issue to project issue
<<include>>
T-UC-1 Update task description, assign task and change task status
<<extend>>
Project Manager
I-UC-2 Add link to RiskManager risk assesment
E-UC-1 Create security event from template
Employee
<<include>>
<<include>>
P-UC-2 Select applicable controls
T-UC-5 Add subissue
<<include>>
P-UC-1 Generate project management SoA
<<include>>
P-UC-3 Save project SoA controls template

Figure 9. ISMS tool functionality

The use case diagram is used for completing ISMS tool functionality descriptions (Section 5.5.1).

Use cases have related to human Actors who participate in the use case as ISMS tool users. Actors can have several roles.

Employee organization member, who can be in the same time in the roles that are described in the business process models, for example, Project Manager, Internal Auditor, Auditee, Relevant manager, Responder, ISMS Authority.

ISMS Authority organization member, who is the project manager of ISMS project (or process manager of ISMS process - depend how organization names it)

Top management - organization member who reviews of ISMS performance

Project Manager organization member who manages projects, could also be organizational process manager

As shown on Figure 9 there is identified 17 preliminary use cases. Use cases are divided into modules by their usage objective: manage issues (T-group), manage security events/incidents (E-group), manage ISMS project (I-group), manage projects and processes (P-group), manage statement of applicability (S-group). The Figure 10 illustrates the use cases dividing into modules.

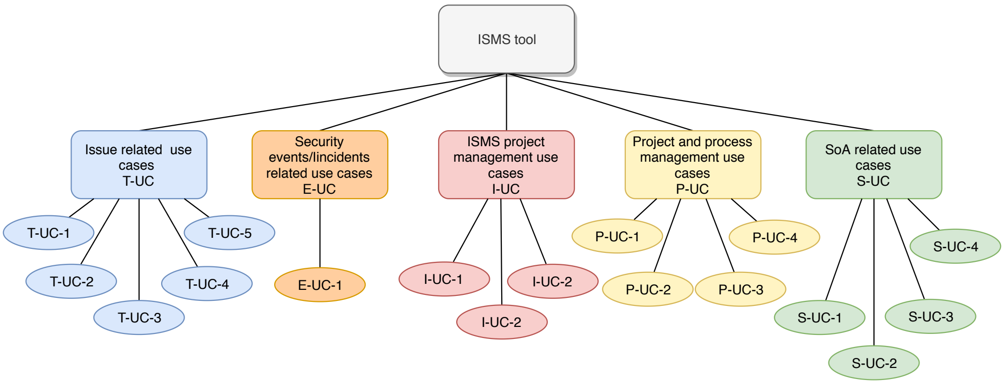

ISMS tool
Issue related use cases T-UC
Security events/incidents related use cases E-UC
ISMS project management use cases I-UC
Project and process management use cases P-UC
SoA related use cases S-UC
T-UC-1
T-UC-2
T-UC-3
T-UC-4
T-UC-5
E-UC-1
I-UC-1
I-UC-2
I-UC-2
P-UC-1
P-UC-2
P-UC-3
P-UC-4
S-UC-1
S-UC-2
S-UC-3
S-UC-4

Figure 10. Modules of the ISMS tool use cases.

Sample use case is detailed in Section 5.5.1. Use cases have natural language descriptions are in Appendix C.6.

5.5.1 ISMS tool functions

ISMS tool functions are described with use case description method using template from [20]. Use case descriptions are used to encapsulate ISMS tool features and to give input for the ISMS tool objects class diagram (Section 5.6). That gives the possibility to describe the dynamics of requirement. The use case description is detailed only in the level needed for the class diagram modeling.

Table 3. Use case P-UC-3

No.	Section	Content
1.	Identifier	P-UC-3
2.	Name	Save template of project SoA controls
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	Medium
6.	Criticality	To define the project based information security management requirements
7.	Source	BP-5 Project management
8.	Short Description	User saves marked project(process) based controls from the ISMS project SoA to use them for the current project and as the template for further created projects.
9.	Goal(s)	G0-9, G0-4
10.	Actor(s)	Project Manager
11.	Precondition	Applicable project/process controls are selected (realised Use case P-UC-2)
12.	Postcondition	Project based SoA template is saved for futher use.
13.	Main scenario	1. System provides to save the result of issues list to be a template. 2. User chooses the issues list to be a "template". 3. System asks the template name and description. 4. User names the template and writes the description of template. 5. System saves the template in the project templates list.
14.	Alternative scenario	2a. User chooses not to save the templete. Proceed to Use case P-UC-2. 2b. User exports the project SoA issues for further templates. 3b. System download the exported SoA issues file. 4b. User names the file and uploads it in project/process description. 5b. System updates the projec/process description.
15.	Related use cases	inclusion of Use case P-UC-2

Use case descriptions are based on this thesis author previous experience.

An example use case is chosen from the module *Project/process management related use cases.* Use case P-UC-3 Save template of project SoA controls description is on the Table 3). This Use case characterizes how the layer-based system could work and how project-based SoA can be specified for the project/process. The example use case is the inclusion of use case P-UC-2.

This use case is core use case of layer-based ISMS tool functionality. Its alternative flows could be decided by the organization or preferred by the ISMS tool administrator.

5.6 ISMS tool components

ISMS tool components are described as class diagram of class objects, also the Jira is an object-oriented solution. ISMS tool requirements matching with Jira features, there is a need to have comparable syntax elements. The primary purpose of the ISMS tool object class diagram (Figure 11) modeling was comparison base of issue tracking tool functionality.

The origin of the classes attributes are the use cases and domain expertise. Defined attributes values can relate some objects, for example, have the same ISO27001 notation number, which enables to filter issues.

In this thesis, class operations are included in the class diagram to implicitly define ISMS tool behavior specified in use cases (Appendix C.6).

Figure 11 illustrates the ISMS tool system objects classes and the relationships of the classes. Object classes descriptions are listed in natural language:

Issue The issue is a requirement to follow by an assignee, who can change issue status, assignee, description and add links. Issue is and object in the Use case T-UC-1, Use case T-UC-2, Use case T-UC-3 , Use case T-UC-4 , Use case T-UC-5 , Use case I-UC-1, Use case P-UC-2

Project Project generalizes different types of projects (all of them are not included on the diagram). Project should have description. Project class has a collection of Issues. Project is an object in the Use case T-UC-3 , Use case I-UC-1, Use case I-UC-3, Use case E-UC-1, Use case S-UC-1, Use case S-UC-2, Use case S-UC-3, Use case S-UC-4 , Use case P-UC-1, Use case P-UC-2, Use case P-UC-3,Use case P-UC-4.

ISMSProject ISMS Project is a project where an organization manages ISO27001 requirements as issues to which in turn are added documents links. ISMS Project improvement needs are subissues of relevant issues. ISMS Project description includes SoA - a fixed version of SoA issue statuses (applicable/nonapplicable) with justifications for nonapplicable issues. This SoA can be used as SoA template to import into projects project-based SoA issues. ISMS Project is and object in the Use case I-UC-1, Use case S-UC-4 , Use case P-UC-4, Use case P-UC-1, Use case P-UC-2, Use case S-UC-1

Business Process Project The project is meant to be a project or process included in the ISMS scope. Project description includes:

1. Information assets (input, output)
2. Requirements to the assets (C, I, A)
3. Related interested parties
4. Regulative, legal and contractual requirements
5. Related non-disclosure agreement (NDA) requirements
6. Relation to controls list template (depends on the project)

These artifacts can be links to the separate documents. This list is incomplete and can differ by internal procedures. SoA issues in the project are importable from SoA template. Non-applicable SoA issues for that project can be marked as non-applicable during the import process. However, these issues require justification in the description field of why they are non-applicable. Business process Project is an object of the Use case I-UC-1, Use case S-UC-4 , Use case P-UC-4, Use case P-UC-1, Use case P-UC-2,Use case P-UC-3

ISMSRiskManager Risk Manager Jira adds-on is developed by SoftComply. RiskManager is an independent object, which have functionality for risk assessment, risk treatment, and verification traceability and risk management model. ISMS Risk manager handles risks in information security management system. Risk Manager is an object in the Use case I-UC-2.

SecurityEventIssue Security Event Issue is a special issue type in incident management project. Security event issues are basing on the issue template. The issue should have Standard notation ID to tie it to Risk Manager. Then it also should be related to SoA project issue trough Standard ID. Issue workflow: ToDo, assess, in progress, evaluate, Done. Security event issue is an object in the Use case E-UC-1.

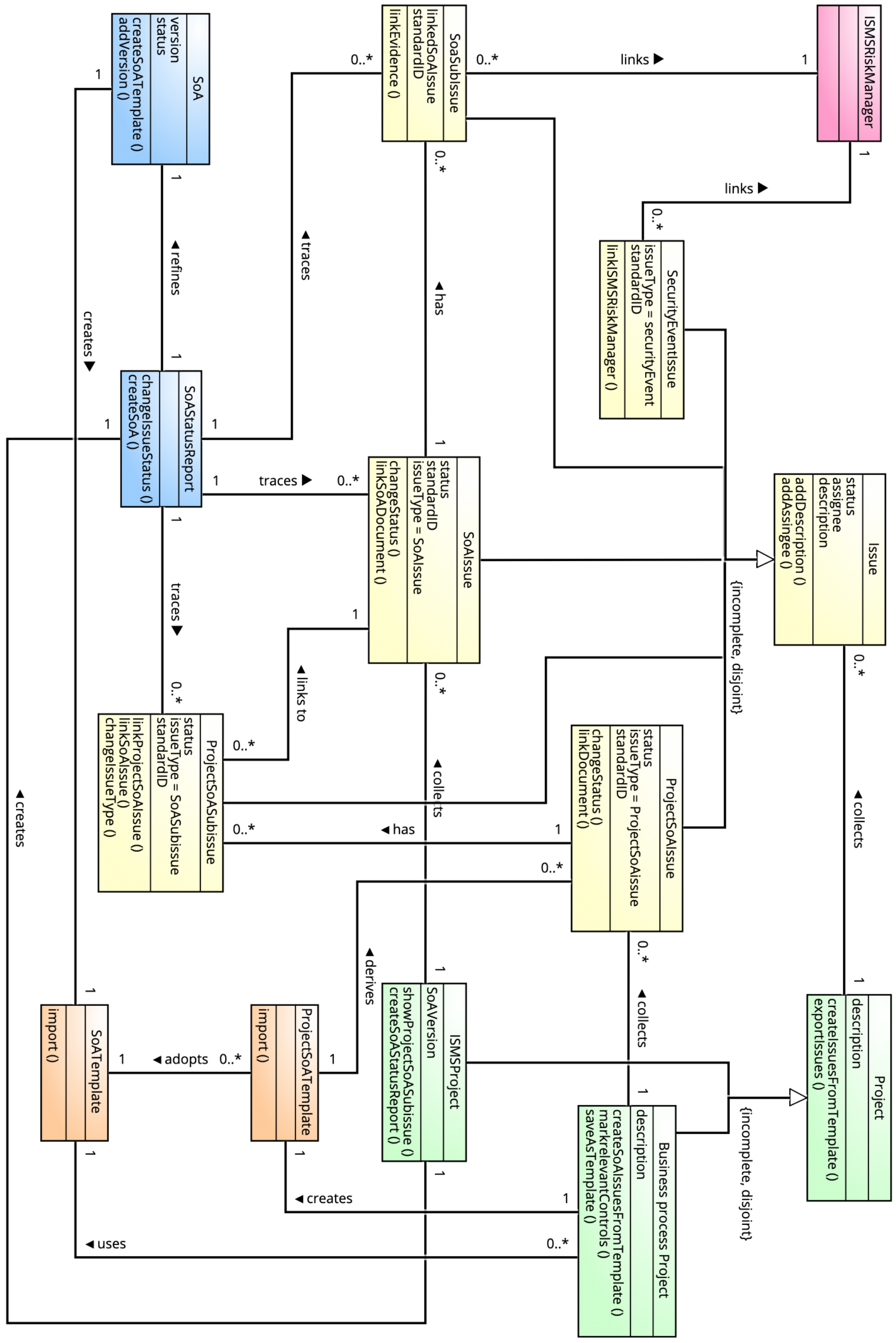


Figure 11. ISMS tool objects class diagram

SoA SoA is a formal version of SoA status report (board). SoA gives an overview of organization decision of applicable and non-applicable ISO27001 and ISO27001 Annex A controls. SoA printable/downloadable version is a base for the template which is used in other projects as SoA issues template. SoA is an object in the Use case P-UC-1, Use case P-UC-2, Use case S-UC-4 , Use case S-UC-1, Use case S-UC-2, Use case S-UC-3, Use case S-UC-4

SoAIssue SoA issue is one-to-one ISO27001 main part or Annex A requirement in ISMS project. SoA issue status is applicable or non-applicable and in case of applicable links required process description and policies. At the very beginning, the status could be as ToDo. If Standard changes, then the status of the issue could be Closed. SoA issue is and object in the Use case T-UC-1, Use case T-UC-2, Use case T-UC-3 , Use case T-UC-4 , Use case T-UC-5 , Use case I-UC-1, Use case P-UC-2

SoaSubIssue SoA subissue is an issue in ISMS project. Subissue is directly related to issue by Standard ID (ISO27001 notation). SoA subissues contain evidence links and decisions to trace ISMS activities. SoA subissue is an object in the Use case T-UC-1, Use case T-UC-3 , Use case T-UC-5 .

SoAStatusReport SoA status report is an overview board of ISMS project subissue statuses. SoA status board report is an object in the Use case I-UC-3,

SoATemplate SoA template is a collection of issues based on ISO27001. Issues statuses are set to be applicable (with relevant links to documents) or non-applicable (with justification). SoA template is generated from the ISMS project issues and contains the SoA version number. SoA template is and object in the Use case I-UC-1, Use case P-UC-3, Use case S-UC-1, Use case S-UC-4

ProjectSoAIssue Project SoA issue is type of project issue which has statuses applicable or non-applicable, its subissues describe using points and evidence of SoA issue implementation in the project. Project SoA subissue is and object in the Use case T-UC-1, Use case T-UC-2, Use case T-UC-3 , Use case T-UC-4 , Use case T-UC-5 , Use case I-UC-1

ProjectSoASubissue Project SoA subissue collects evidence of how this project manages parent issues requirements and rules. Project SoA subissue is and object in the Use case T-UC-1, Use case T-UC-2, Use case T-UC-3 , Use case T-UC-4 , Use case T-UC-5 , Use case I-UC-1

ProjectSoATemplate Project SoA Template is a collection of SoA issues relevant to the specific type of projects. Project SoA template bases on SoA, where non-applicable issues are marked to be non-applicable and other issues are to manage and to produce evidence of the performace. Project SoA template is and object in the Use case I-UC-1, Use case P-UC-3, Use case S-UC-1, Use case S-UC-4

5.7 Summary

Section described analysis and systematization of ISMS management process for ISMS tool functionality. Also requirements for issue tracking system are presented as class diagram. Outcome of this Section can be used for an input for configuring Jira for ISMS management. ISMS management business process flows are included. The outcomes of this Section are the input for next validation section.

6 ISMS tool specification validation

Thesis idea and specificatin was verified during interviews with possible stakeholders in two phases: in planning phase and in specification validation phase. ISMS tool specification and ISO27001 requirement coverage was verified by matching standard clauses with analysis results.

6.1 Preliminary interviews

During the planning phase of this thesis were conducted ten interviews. The thesis author participated or conducted eight of them. Some of the interviews were done as a part of the "Software product management II" course group work [24]. The group work purpose was to understand the market needs of the product. Interviews were made with users (from private and public sector), ISMS auditor and SoftComply CTO (certified Jira expert).

Interviewees of the software development field and hosting service provider were interested in this product. They are using the Jira platform provided by Atlassian. They prefer that there are no more special tools used for ISMS management, and all issues are in a single platform, part of management system. This discussion supports the Section 3 results.

Feedback of manufacturing field representative explained, that their domain organizations do not use Jira nor other issue tracking solutions usually and prefer special compliance tool for ISMS, managed by a single person.

ISMS auditor was interested about traceability. It is important to notice, that auditor is not the user of the ISMS tool. An auditor needs the evidence of the ISMS performance. Organizations must provide evidence with or without tool. Tool itself is not essential for the auditor.

Jira expert wanted more details about the layer-based ISMS tool requirements to understand needed functionality and processes. Then it is possible to evaluate the proof of concept of the ISMS tool realization on Jira and integration with RiskManager (developed by SoftComply).

These interviews directed starting point of the layer-based ISMS tool specification.

6.2 ISMS tool specification validation

ISMS tool specification was ready for validation on April 2019. The validation was carried out in the form of interviews, providing review and walk-through information about ISMS tool specification artifacts (see Section C).

6.2.1 ISMS manager interview

For ISMS manager interview, the thesis author introduced the ISMS tool idea, discussed ISMS tool goals and walked through the ISMS tool business processes. The user was public sector representative, security and ISO27001 and ISKE specialist, Jira user. In her organization, ISKE was implemented, and implementation of the ISO27001 was initiated. Organization manages some security issues in Jira and tracks some security requirements in specially developed tool.

ISMS manager evaluated the layer-based ISMS model to be feasible for implementation. The main idea was understandable and integration with RiskManagement was very honorable. Selected questions discussed:

Questions: How to add ISKE requirements into the same system?

Answer: Issues are possible to import. If there is a mapping between the ISKE and ISO27001, then it is possible to manage them with the help of ISMS tool functionality. If the user wants to filter ISKE issues separately from ISO27001 issues, then the user should add a custom field to ISKE issues (for importing the issues: Use case I-UC-1; supporting scalability G0-9).

Question: How is managed the versions of new SoA?

Answer: SoA version numbers should be related to SoA templates. Additional field with SoA version info should be added to issues (update needs Use case S-UC-3; supporting maintenance G0-2).

Question: What happens when SoA changes during the project?

Answer: This user story should be specified. Manually is possible to follow the changes in SoA template and update project SoA issues based on that (Use case P-UC-1 needs improvement; support G0-8).

The main concerns were related about ISMS tool concept were related with the organization culture and reluctance for changes. The suggestion for that could be only management commitment (specified in ISO27001 standard clause 5, see Section 4) and positive example. Suggestion was made to include screenshots with realisic examples into the user manual.

6.2.2 Jira expert interview

Jira expert (SoftComply CTO) was briefed about the layer-based ISMS tool idea using specification. ISMS tool goals were mentioned. Object of the discussion was layer-based ISMS tool class diagram (Figure 11), its review and evaluation. Jira expert is responsible for continuous integration and the development of SoftComply products using Jira and other Atlassian products. He had worked with Atlassian products from 2013. Expert has earned Atlassian Certified title in Agile Development with Jira Software.

Table 4. ISMS tool specification coverage of the ISO27001 requirements

	ISO27001 clauses						
	4	5	6	7	8	9	10
Business processes	BP-1, BP-2	BP-1, BP-2, BP-7	BP-2, BP-5, BP-6, BP-7	BP-1, BP-2, BP-5, BP-6, BP-7, BP-8	BP-1, BP-3, BP-4, BP-5	BP-2, BP-5, BP-6, BP-7, BP-8	BP-1, BP-2, BP-6
Use cases	T-UC-1, T-UC-2, T-UC-5, I-UC-1, I-UC-2, I-UC-3	T-UC-1, T-UC-2, T-UC-5, I-UC-1, I-UC-2, I-UC-3, S-UC-1, S-UC-2, S-UC-3, S-UC-4	T-UC-1, T-UC-2, T-UC-4, T-UC-5, E-UC-1, I-UC-1, I-UC-2, I-UC-3, P-UC-1, P-UC-2, P-UC-3, P-UC-4, S-UC-1, S-UC-2, S-UC-3, S-UC-4	T-UC-1, T-UC-2, T-UC-4, T-UC-5, E-UC-1, I-UC-1, I-UC-2, I-UC-3, P-UC-1, P-UC-2, P-UC-3, P-UC-4, S-UC-1, S-UC-2, S-UC-3, S-UC-4	T-UC-1, T-UC-2, T-UC-3, T-UC-4, T-UC-5, E-UC-1, I-UC-2, P-UC-1, P-UC-2, P-UC-3, P-UC-4	T-UC-1, T-UC-2, T-UC-4, T-UC-5, E-UC-1, I-UC-1, I-UC-2, I-UC-3, P-UC-1, P-UC-2, P-UC-3, P-UC-3, S-UC-1, S-UC-2, S-UC-3, S-UC-4	T-UC-1, T-UC-2, T-UC-5, I-UC-1, I-UC-2, I-UC-3
Class Diagram Classes	Issue, Project, ISMSProject, BPP, ProjectSoAIssue, ProjectSoATemplate	Issue, Project, ISMSProject, BPP, ProjectSoATemplate	Issue, Project, ISMSProject, BPP, ISMSRiskManager, SecurityEvent, SoA, SoAIssue, SoASubissue, ProjectSoAIssue, ProjectSoASubIssue	Issue, Project, ISMSProject, BPP, SoASubissue, ProjectSoASubIssue	Issue, Project, ISMSProject, BPP, ISMSRiskManager, SecurityEvent, SoASubissue, SoATemplate, ProjectSoAIssue, ProjectSoASubIssue, ProjectSoATemplate	Issue, Project, ISMSProject, BPP, ISMSRiskManager, SoASubissue, SoAStatusReport, SoATemplate, ProjectSoASubIssue	Issue, Project, ISMSProject, BPP, ISMSRiskManager, SoASubissue, SoAStatusReport, ProjectSoASubIssue

After the class diagram detailed review his evaluation conclusion was that there are no obstacles to implement the layer-based ISMS tool using Jira features. Questions arose concerning how to import and export project issues with selected issue fields (described Use case P-UC-1 and Use case I-UC-1). Additional research on available Jira add-ons is recommended. The discussion was about how to capture the ISMS tool into a product because the specified ISMS tool is not an add-on, but the configuration is complex, and users prefer pre-configuration package. Implementation of specified ISMS tool is possible without additional software development.

General comments: name of the components can be confusing for users and should be reviewed for clarity. Using Jira issue standard fields should be avoided, as it may interfere organization agreed workflow.

Additional questions were:

Questions: Does the user need so much freedom? There are many possibilities to direct the user to use the tool features only in one way.

Answer: At this ISMS tool specification phase had been in focus only needs for abilities, no constraints. Restrictions should be specified in the future.

Question: SoA versions should be defined in every SoA Issue. Otherwise, the versions of SoA would not be traceable.

Answer: Additional custom fields for the issue should be added and specified (Use case S-UC-3 needs improvement).

The specification is ready to do the configuration plan and start the ISMS tool test configuration.

6.3 Specification completeness validation

ISO27001 does not accept exclusion from the standard clauses 4-10. To check the completeness of the specification Table 4 is compiled. Table presents ISO27001 clauses vertically and specification artifacts horizontally. Tabel confirms that ISO27001 clauses 4 - 10 are included into specification.

6.4 Summary of validation

Interviews revealed that models, visualizations and diagrams are most valuable to introduce and explain layer-based ISMS management processes and tool principles. Jira administrators were using class diagram to understand and validate proposed solution. Persons responsible for ISMS implementation found BPMN models most useful and clear to evaluate layer-based ISMS tool suitability for their organizations and processes.

Interviewees understood the concepts of layer-based ISMS tool and evaluated that the Jira platform is appropriate platform to use for information security management as a natural part of organization management system. Jira expert confirmed that Jira enables the specified object classes and their operations depicted in the layer-based ISMS tool class diagram.

Suggestions were made to improve layer-based ISMS tool in upcoming phases:

- to predefine more custom fields and avoid fields defined by Jira core functionality;
- to define mandatory workflow with constraints to users;
- to find better names to object classes and fields (to simplify the understanding);
- to prepare the test configuration and configuration guide;
- to play through the full process and include screenshots with realistic examples to the user manual.

The validation confirmed that at the proof of concept level the layer-based ISMS tool specification can be used for implementation. Layer-based ISMS tool covers ISO27001 requirements.

7 Thesis summary

The result of the thesis is ISO27001 compliant layer-based ISMS tool requirements specification in the level to get the proof of concept validation, that issue tracker tool Jira can be used as a platform for ISMS management. The main idea of the specified layer-based ISMS tool is to use ISO27001 compliant organization statement of applicability (SoA) as a template for the organization's other projects/processes management as a predefined security layer. That security layer assures the scalability, integration and traceability of ISMS performance.

7.1 Limitations

Thesis results are not used in any real ISMS management processes for ISO27001 implementation yet. Layer-based ISMS tool specification is provided in a proof-of-concept level so, that it can be adjusted to the organization's needs.

Proposed layer-based ISMS tool specification requires to use third-party components to fulfill risk management requirements specified in ISO27001.

7.2 Answers to research questions

This thesis research questions were:

1. How to manage an ISO27001 based information security management system using issue tracking tool, for example, Jira?
   (a) What are the ISO27001 processes of the layer-based ISMS tool to manage and trace?
   (b) What are the required issue tracking tool functionalities to implement layer-based ISMS tool?
   (c) How to systematize and visualize layer-based ISMS solution requirements?

Question (a) was answered in the Section 5.4 with modeling the business processes of layer-based ISMS. The answer to the question (b) is given in Section 5.5.1, where ISMS tool's fuctionality was described in a form of use cases.

Jira functionality requirements, for answering question (c), are visualized on Figure 11, ISMS tool objects class diagram.

Layer-based ISMS tool functionality analysis provides process descriptions and input on how to manage ISMS using issue tracking. Jira issue tracking system configuration can be implemented following the systematized use case and class diagrams. This answers to the research question (1.).

7.3 Conclusion and future work

The specification validation resulted with the conclusion, that with expert knowledge it is possible to configure Jira projects, issues and board to support ISMS management on Jira platform. It would be preferable to have the ISMS tool for Jira platform as predefined configuration package. The further work with the specification could continue with configuring the Jira for the ISMS management, testing the usability and improving on some questions that arose from the validation process. The final result would be the layer-based ISMS tool for the private and public sector organizations.

References

[1] Buldas,A., Oit, M., Praust, V.: Turvaklasside kirjeldused. Tehniline aruanne. Dok. DO–X-09-0498. Küberneetika AS (1998)

[2] Fowler, M.: UML Distilled: A Brief Guide To The Standard Object Modeling Language. Pearson Education,Inc., 3rd edition (2004)

[3] Guidance and gaps analysis for European standardisation. Privacy standard in the information security context. ENISA. (2019)
`https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation`
Last access: 13.04.2019.

[4] Hanson, V., Praust, V.: Infosüsteemide turbe etalonmeetmete süsteemi koostamine. Aruanne. Dok. CY-AA-A-054-031029. Cybernetica AS (2003)

[5] Horkoff, J., Dalpiaz, F., Franch, X.: iStar 2.0 Language Guide (2016)
`https://arxiv.org/pdf/1605.07767v3.pdf`
Last access: 02.05.2019.

[6] Hughes, B.,Cotterell, M.: Software Product Management. McGraw-Hill Education, 5th edition (2009)

[7] Humphreys, E. T.: Information system management system standards. In: SC 27 security techniques. 25 years of Information security Standardisation (1990-2015), pp.56–73. ISO/IEC (2015)

[8] Infosüsteemide kolmeastmelise etalonsüsteemi ISKE. rakendusjuhend. RIA (2017).
`https://www.ria.ee/sites/default/files/content-editors/ISKE/iske_rakendusjuhend.pdf`
Last access: 22.03.2019.

[9] International Standard ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization, iso.org (2013)

[10] ISKE portaal, RIA (2019)
`https://iske.ria.ee`
Last access: 13.04.2019.

[11] ISO/IEC JTC 1/SC 27 Information Security, cybersecurity and privacy protection. International Organization for Standardization, iso.org (2019)

https://www.iso.org/committee/45306.html
Last access: 13.04.2019.

[12] International Organization for Standardization.All about ISO. International Organization for Standardization, iso.org (2019)
https://www.iso.org/about-us.html
Last access: 15.05.2019.

[13] IT-Grundschutz-Kompendium – Edition 2019. BSI (2019)
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html
Last access: 13.04.2019.

[14] Maciaszek, L. A.: *Requirements analysis and system design.* Pearson Education Limited, second edition edition (2005)

[15] Jira Product Guides and Tutorials. Atlassian (2019)
https://www.atlassian.com/software/jira/guides/getting-started/overview
Last access: 16.05.2019.

[16] Market Share / Project Management / Jira. Datanyze (2019)
https://www.datanyze.com/market-share/project-management/jira-market-share
Last access: 01.05.2019.

[17] Milani, F.: Digital Business Analysis. Springer Nature Switzerland (2019)

[18] NCSI National Cyber Security Index. e-Government Academy.(2019)
https://ncsi.ega.ee
Last access: 13.04.2019.

[19] Pimentel, J., Castro, J.: piStar Tool – A Pluggable Online Tool for Goal Modeling. 2018 IEEE 26th International Requirements Engineering Conference, pp 498–499. IEEE (2018).

[20] Pohl, K.: Requirements Engineering.Fundamentals, Principles, and Techniques. Springer (2010)

[21] Risk Manager User Manual. SoftComply (2019)
https://softcomply.com/softcomply-risk-manager/softcomply-risk-manager-user-guide/
Last access 13.05.2019

[22] Schmuller, J.: Sams teach Yourself UML in 24 Hours. Sams Publishing, 3rd edition (2004).

[23] Seeba, M.: ISO27001 ja ISKE võrdlustabel. Dok A-5-7. Cybernetica AS (internal document) (2014)

[24] Seeba, M., Burget, M., Kikerpill, L.: University of Tartu: Software Product Management 2. Groupwork reports. (2019)

[25] Seeba, M., Kalu,A., Pruulmann-Vengerfeldt, J.: ISKE tööriista täiendamise ettepanekute analüüs. Dok. A-87-1. Cybernetica AS, Procurer and Copyright RIA (2014)

[26] Smartlink OÜ: ISKE rakendustööriista analüüs. RIA (2010)

[27] Tepinfo OÜ: ISKE rakendustööriista analüüs. RIA (2007).

[28] The ISO Survey of Management System Standard Certifications – 2017 – Explanatory Note. International Organization for Standardization, iso.org (2018)
`https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/00._Overall_results_and_explanatory_note_on_2017_Survey_results.pdf?nodeid=19208898&vernum=-2`
Last access: 20.03.2019.

[29] Three-level IT Baseline Security System ISKE, RIA (2019).
`https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html`
Last access: 13.04.2019.

Appendices

A Glossary

Board A board displays issues from one or more projects, giving to the user a flexible way of viewing, managing, and reporting on work in progress in Jira [15].

ISKE Estonian information security baseline system

ISMS Information Security Management System. In this thesis used as synonym for ISO27001 compliance management system

ISO27001 International Standard ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements [9]

Issue A Jira 'issue' refers to a single work item of any type or size that is tracked from creation to completion. For example, an issue could be a feature being developed by a software team, a to-do item for a marketing team, or a contract that needs to be written by a legal team [15].

Project A project (in Jira) is a collection of issues that are held in common by purpose or context. Issues grouped into projects can be configured in a variety of ways, ranging from visibility restrictions to available workflows [15].

SoA Statement of applicability is the list of controls and justification for inclusions and the justification for exclusions from ISO27001 normative Annex A adapted by organization [9].

Workflow Workflows in Jira represent the sequential path an issues takes from creation to completion [15].

Workflow management tool Synonym for issue tracking tool in context of this thesis.

B Modeling methods of layer-based ISMS tool

Appendix describes methods used for layer-based ISMS tool analysis. Information is included for audience who does not have active expertise on different modeling languages.

Subsection titles are kept in sync with specification in Appendix C.

B.1 ISMS tool goal analysis

A goal is an intention with regard to the objectives, properties, or use of the system[20]. This specification goal modeling is made in high level to show the product and organization strategy realted with ISO27001.

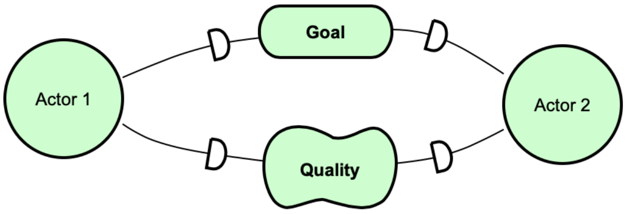


Figure 12. i* components used for ISMS goal modelling

For goal modeling i* (i-star) modeling language [5] is used to reason *who?* and *why?* needs the ISMS tool. The goal modeling is made on high level to show the product and organization strategy related with ISO27001.

There are many tools listed on the i*Wiki[9]. For this study was chosen PiStar tool. i* modeling language tool PiStar [19] helped to illustrate the ISMS tool goals on figures. The PiStar is online tool what does not require special access account what simplifies its usage. It is with simple interface and helpful hints. There is possible to download your work to upload and continue when ever user needs[10].

The idea of the i* modeling langugage is to show the dependencies between Actors. Dependency directions are shown on the line with character "D". For example (see Figure 12) Actor 1 depends on Actor 2 to archive the Goal and also to achive the quality.

On the models the organization is shown as one Actor. The Actor decomposition is managed on business process modeling Section (see Section C.4).

[9] `http://istar.rwth-aachen.de/tiki-index.php?page=i%2A+Tools&structure=i%2A+Wiki+Home` Last access: 21.04.2019

[10] `http://istar.rwth-aachen.de/tiki-index.php?page=piStar` Last access 21.04.2019

Each goal has its unique ID-s (starting with "G") which are shown on figures and also mentioned in specification textual part of use case descriptions (see Section C.6).

The goal model is based on ISO27001 textual analysis. The output of the goal modeling gave the direction, which kind of functionality should be realized with ISMS tool features.

B.2 ISMS process analysis

Business process modeling of layer-based ISMS tool is implemented in Business Process Modeling Language (BPMN). BPMN gives the visualization of the processes intuitively to understand by users and non domain specialist. These models can be used as a base material to introduce the whole process of ISMS implementation. For modeling were used the basic components of BPMN notation to keep models simple as possible. The used components with descriptions of usage are illustated on Figure 13.

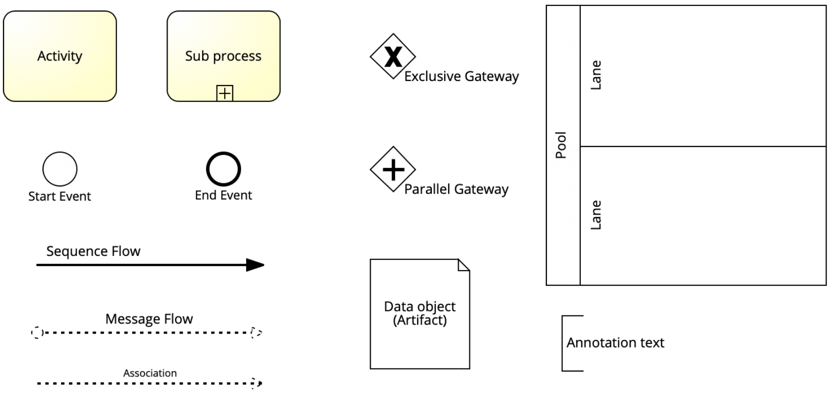


Figure 13. BPMN components used for ISMS processes modeling

The detailing level of the represented business process models is chosen by the need for ISO27001 text and human activity tasks. Each organization can add to the models of its specific stakeholders or detail actions by their own needs. The process of composing the models was divided into two phases: at first, was modeled the human activities what satisfied the ISO27001 requirements and goals; in the second phase were added ISMS tool specific activities into a separate pool. Then were added message flows between Organization and ISMS tool activities.

The processes describes logical sequence: establish, implement, maintain and improve. Processes are iterative in some parts or entirely.

For input of the business process analysis is used the ISO27001 text and the thesis author domain expertise to investigate the processes to be compliant with ISO27001 requirements. The layer-based ISMS model idea was the result of this phase.

For business process analysis is used as an input the ISO27001 standard text and the specification author domain expertise to investigate the processes to be compliant with standard requirements. Additionally is analyzed a general project management process from textbook [6] as an example of a business process in the organization. To every process-model is added ISMS tool pool to show the expectations of the tool (basing on goal analysis).

For visualization is used online tool named Signavio[11].Tool is specialized for process modeling and analyst work effectiveness. Main reason to use the special modeling tool (not any drawing tool) was the ability to use tool dictionary and optimize the modeling process (making textual changes on one model, it automatically distributes the change to related models). Signavio usage motivation based on its free usage by academic license. The thesis author obtained the license as a student of the University of Tartu.

B.3 ISMS tool functionality

Use case diagram were used for specifying the ISMS tool use cases and the use cases relationship. The use case diagram captures use cases on one view and shows the relationship of Actors and ISMS tool each use case.

Based on the business process analysis (see Section C.4), each modeled activity in the ISMS tool pool was analyzed separately to find similarities and the need to have the use case(s). The result was ISMS tool use case diagram that shows the needed system functionality of ISMS tool (see Figure 30). For traceability, each use case description has a reference to the business process as a source of the use case.

Use case diagram uses UML *(Unified Modeling Language)* use case diagram components illustrated on the Figure 14. On the diagram there are human Actor who interact with system (it this thesis: ISMS tool). Human Actor associates with concrete Use Case(s). Use case may include other Use Case(s) [2].

The ISMS Use Case diagram is the input to complete the Use Case descriptions (see in Section C.6).

Use case diagram were modeled with Signavio tool. Signavio provided to use the defined activities from modeled Business Processes to model the Use case diagram. That was enabled trough the Signavio dictionary functionality.

[11] `https://www.signavio.com` Last access: 15.05.2019

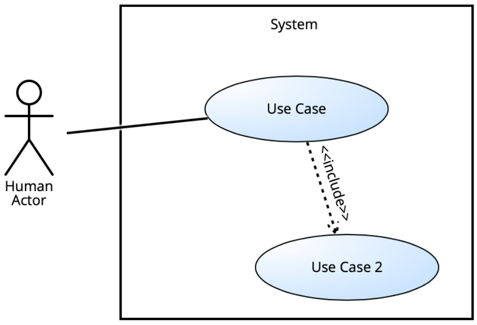


Figure 14. UML components used for ISMS funtionality modeling

B.4 ISMS tool functions

Use case is the flow of the events in the natural language. There is no standard for use case description. Different textbooks suggest different templates [2].

ISMS tool functions are described with use case description method using template from [20]. Use case descriptions are used to encapsulate ISMS tool features and to give input for the ISMS tool objects class diagram (Section 5.6). That gives the possibility to describe the dynamics of requirement. The use case description is detailed only in the level needed for the class diagram modeling.

Use case descriptions are based on this specification author previous experience. In the Section C.6 are described 17 use cases in tabled form.

B.5 ISMS tool components

For undestanding the concept of UML class diagram modeling and motivation to use this method for this specification is based on textbooks [2], [14], [20].

ISMS tool components are described as class diagram of class objects, also the Jira is an object-oriented solution. ISMS tool requirements matching with Jira features, there is a need to have comparable syntax elements. The primary purpose of the ISMS tool object class diagram (Figure 11) modeling was comparison base of issue tracking tool functionality.

Class diagram identifies ISMS object classes, their attributes, operations and relationships.

The components used on class diagram for modeling ISMS tool classes are illustrated on the Figure 15.

Each class has attributes. Attributes declare classes [14]. The origin of the classes attributes are the use cases and domain expertise. Defined attributes values can relate some objects, for example, have the same ISO27001 notation number, which enables to filter issues.

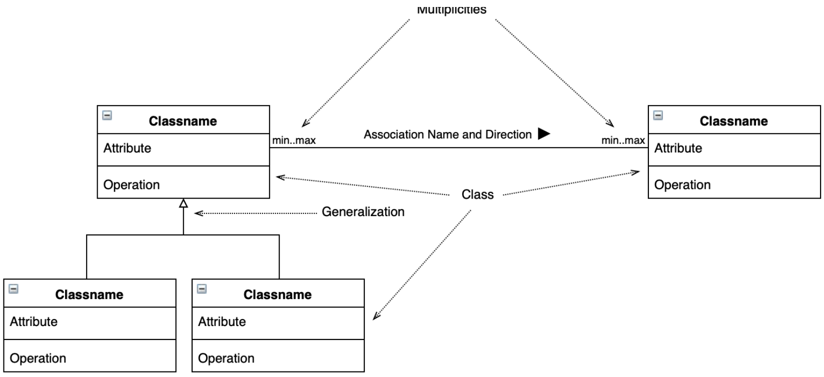


Figure 15. UML class diagram components used for ISMS components modeling

Classes are static structures. However, the operations of the classes fulfill the dynamic behavioral requirements of ISMS tool specified in use cases (see Section C.6).

Associations between classes establish pathways for collaboration.The multiplicity is the property of association. It indicates the permissible number of values that can be assigned to the class objects (the minimum and maximum values) [14]. In this specification class operations are included into class diagram to implicitly define the ISMS tool behavior.

In this thesis, class operations are included in the class diagram to implicitly define ISMS tool behavior specified in use cases (Appendix C.6).

In this specification, class operations are included in the class diagram to implicitly define ISMS tool behavior specified in use cases (Appendix C.6).

For modeling was used tool named Signavio which supported to follow the syntax.

C ISMS tool specification

In this Section is specified the ISMS tool requirements defining the layer-based ISMS tool goals, required business processes, functions and ISMS tool components. The specification target group is a product manager and ISMS implementer who plans to use Jira for ISMS management.

C.1 Scope

The scope of the specification focuses on specifying the ISO27001 requirements from its clauses 4 to 10. The standard ISO27001 Annex A is taken into account on the aggregated level. Every organization designs its specific security objectives and measures given in ISO27001 Annex A each control. The study does not constrain the Annex A controls implementation.

This thesis does not cover following ISMS components: risk management, asset management, and document management. These components are existing add-ons of Jira and can be used to implement full-scale ISMS.

Jira core functionality is used to implement ISMS tool functionality. Focus is to understand which functionality from the Jira is required for ISMS. The context interfaces related with ISMS tool are illustrated on Figure 16.

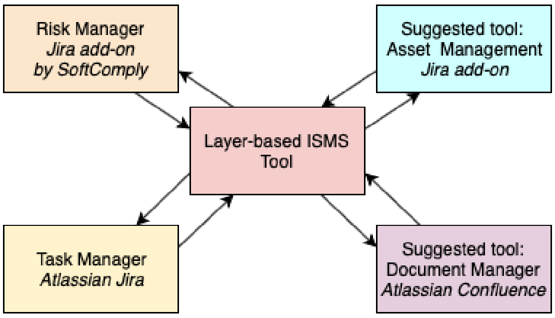


Figure 16. Related products of ISMS tool.

ISMS tool is positioned in the center of the Figure 2. On this thesis view, surrounding parts are mandatory for ISMS adoption. This study does not consider integration requirements of these products. It is assumed that these products are possible to integrate through linking the relevant object to the ISMS project issues. In the specification there is explicitly shown the linkage to Risk Management tool.

C.2 ISMS tool goal analysis

Goal modeling is made at high level to show the product and organization strategy relation to ISO27001.

Figure 17 illustrates who are the Actors (stakeholders) of the ISMS implementations and what are their interests. Organization internal goals to be achieved are shown separately. This model visualizes *who* and *why* they participate in the scope of ISMS of organization.

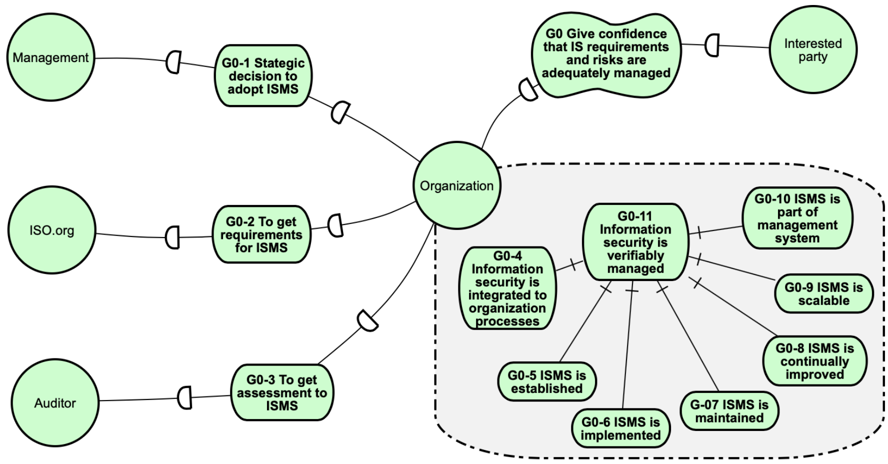

Management
G0-1 Stategic decision to adopt ISMS
G0 Give confidence that IS requirements and risks are adequately managed
Interested party
Organization
ISO.org
G0-2 To get requirements for ISMS
G0-11 Information security is verifiably managed
G0-10 ISMS is part of management system
G0-4 Information security is integrated to organization processes
G0-9 ISMS is scalable
G0-8 ISMS is continually improved
G0-5 ISMS is established
Auditor
G0-3 To get assessment to ISMS
G0-6 ISMS is implemented
G-07 ISMS is maintained

Figure 17. G0 ISMS goals.

The second Figure 18 illustrates the ISMS tool goal dependencies focusing on organization with the same Actors of detailed specification Figure 17. On the Figure 18 there is added an Actor – the ISMS tool, the focus point of this specification. The figure shows which goals should be managed with ISMS tool (colored in violet). These goals are G0-2, G0-4, G0-9, G0-10, G0-11. Special attention is on the direction of the goals - ISMS tool needs the requirements to be defined by organization (G0-2). The ISMS tool quality depends on that. Goals G0-5, G0-6, G0-7 can be melted into other goals as gathering the evidence of ISMS performance. The processes itself should be done by organization.

On the figure there are actors mentioned in the ISO27001 standard clauses 4 to 10: (i) **Organization** itself as an entity (the organization as Actor decomposition is managed on business process modeling (see Section C.4)), (ii) **Interested party** (any external entity whose interest is that the organization manages his information security adequately), (iii) **Management**, (iv) **ISO.org** who provides the ISO27001 standard and its requirements and (v) **Auditor** who can be internal or external auditor in this context.

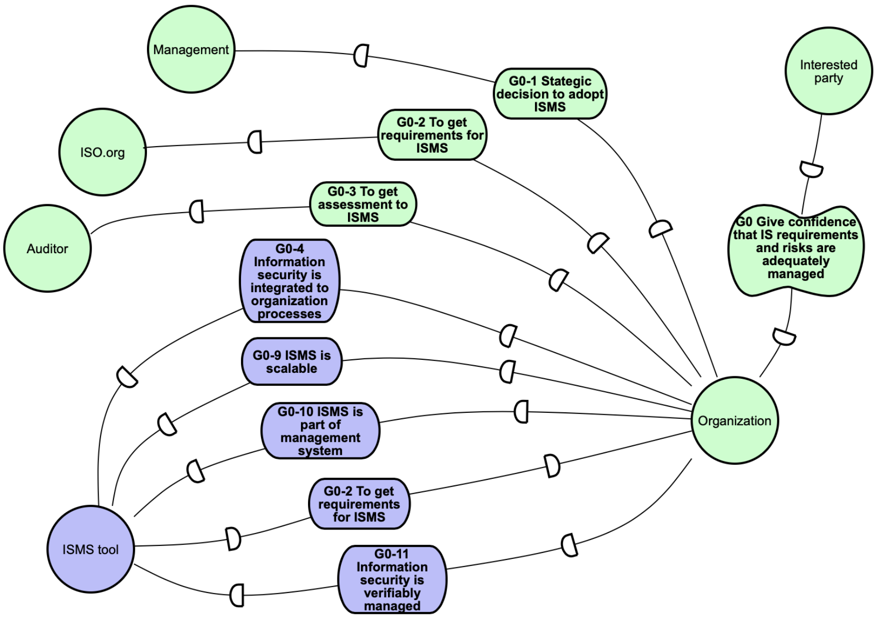

Management
ISO.org
Auditor
Interested party
G0-1 Stategic decision to adopt ISMS
G0-2 To get requirements for ISMS
G0-3 To get assessment to ISMS
G0 Give confidence that IS requirements and risks are adequately managed
G0-4 Information security is integrated to organization processes
G0-9 ISMS is scalable
G0-10 ISMS is part of management system
G0-2 To get requirements for ISMS
G0-11 Information security is verifiably managed
Organization
ISMS tool

Figure 18. ISMS tool goals.

ISO27001 standard defines the goals for the organization ISMS (see also Section 4.2). Goals can be listed as follows [9]:

G0 ISMS gives confidence to interested parties that the organization manages the risks adequately – interested party can trust the organization who can prove that ISO27001 requirements are adapted

G0-1 ISMS implementation is strategic decision – the top management is interested in the successful ISMS implementation and gives his commitment to that

G0-2 ISMS is based on ISO27001 requirements

G0-3 ISMS is assessable – compliance assessment to ISO27001

G0-4 ISMS is part of and integrated with the organization's processes and overall management performance – processes under the scope of ISMS are adapted to use information security rules, but also the opposite way - ISMS should be implemented into the existing procedures and processes

G0-5 ISMS is established – organization knows its information security requirements and context, risk assessment is done, procedures are designed

G0-6 ISMS is implemented – information security policies and processes are communicated and functioning

G0-7 ISMS is maintained – information security policies and processes performance is monitored and measured

G0-8 ISMS is continually improved – information security policies and processes functioning monitoring and measuring results are evaluated and refined based on risk assessment

G0-9 ISMS is scalable following the needs of the organization – the organization can change its processes, organization structure, grow or decrease but still is able to take into account information security requirements in defined level based on risk criteria

G0-10 ISMS is a part of management system – information security is supporting business objectives and taken info account when planning business objectives

G0-11 ISMS is verifiably managed – there are documented evidence of information security management performance

ISMS tool goals can be concluded that ISMS tool main purpose is to help scalably integarate ISMS into organization processes and trace activities to get evidence as a natural part of organization management system.

C.3 Description of the layer-based ISMS tool concept

Layer-based ISMS enables to bring information security requirement systematically into projects and processes, where an organization should implement ISMS. So it is possible to distribute the knowledge of information security over hole organization in required form implicitly. Statement of Applicability (SoA) is the central distribution artifact of layer-based ISMS. Every project and process can adapt itself to produce its SoA compliant to organization SoA. Any time the organization can monitor centrally the status of information security. Layer-based ISMS model integrates information security visibly into processes and projects. It is merely scalable and relates organization staff into ISMS in the most natural way.

Figure 5 illustrates the layer-based information security management solution concept, which should be supported by processes. Information security requirements and controls together with risk management direct the organization statement of applicability (SoA). SoA contains the principles how ISMS should be implemented. These principles need to be spread to organization projects/processes. The layer-based information security enables to use the same SoA template to adopt it for each project/process. The feedback system works through the security events or

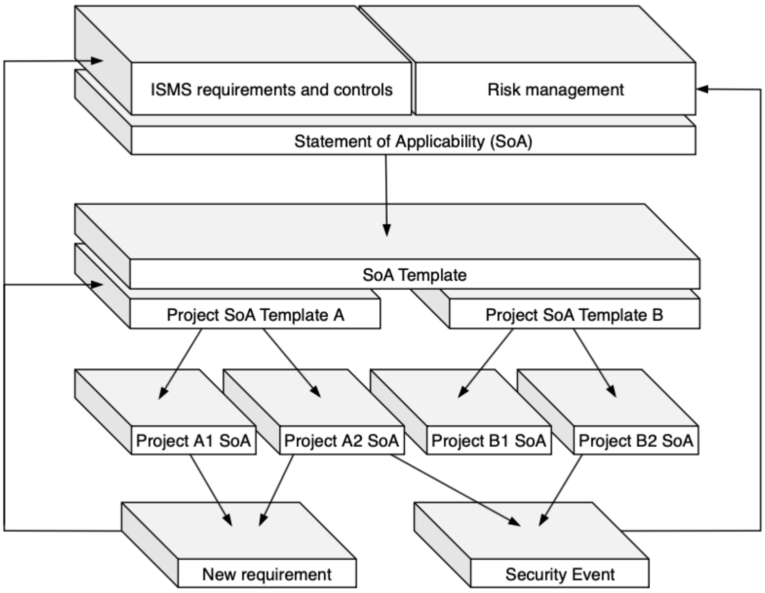


Figure 19. Layer-based information security management

new and changed requirements as an input to risk management and organization context analysis.

Each process and/or project can adapt and track SoA issues with adding specific details or excluding some non-applicable issues. Central ISMS project gathers evidence of security requirements implementation in processes and projects through reports and board functionality.

C.4 ISMS processes analysis

For organization compliance with ISO27001 requirements, standard does not accept any exclusions from the Clauses 4 to 10 [9]. General model of business processes of ISMS are on Figure 20. There are defined eight sub-processes.

They are chosen by the principle, that they cover standard mandatory clauses.

The ISMS general view (see Figure20) gives the understanding of the subprocesses relationship to each other and the sequence. It also contains the primary input and output documents. Actors are not specified in this model as it is the general view. Input of general process is the strategic decision to implement ISMS in the organization (G0-1). This decision is also the starting trigger. The output of the process is documented evidence (G0-11) that can give the verification of ISMS establishment (G0-5), implementation (G0-6), maintenance (G0-7), and improvement(G0-8). The process should end on the case the management decides not to continue with ISMS.

Next are described subprocesses of ISMS general business model.

BP-1 Define information security policy The purpose of the information security policy is to give the directions of organization information security what are aline with organization business strategy and takes into account internal and external requirements [9]. Information security policy related business process (see Figure 21) flows throughout the ISO27001 clauses: 4.1, 4.2, 4.3, 5.1, 5.2, 7.4, 8.3 and 10.2. Also covers ISO27001 Annex A controls under A.5. The trigger of the process is the decision to adapt ISMS in the organization (G0-1). The actors of the process are the ISMS Authority and Management. The input to generate the information security policy to the organization are ISO27001 requirements, interested party requirements, legal and regulatory requirements and contractual obligations (G0-2). The output of the process is (new version of) information security policy, ISMS scope (G0-5, G0-11).

BP-2 Compile SoA first version SoA preliminary version compiling (see Figure 22) is layer-based ISMS tool specific business process with the purpose to give input to other projects and issues and to keep under control ISMS related issues. This process is based on ISO27001 clauses: 6.1.2, 6.1.3, 5.3, 4.4, 7.5, 9.1, 10.2. Also,this process covers controls of the ISO27001 Annex A on the way that it manages these controls. The starting point of the process is the existing decision to adapt ISMS and information security policy is defined. Then there is a need for next steps what organization manages under the ISMS project. So the process starts with creating ISMS project. The input of compiling the SoA are ISO27001 (with its requirements), information security policy and ISMS scope, risk assessment, and existing internal policies, procedures, and processes. The output of the process is the SoA status report that contains links to related documents and issues (G0-5, G0-11).

BP-3 Defining subpolicy Subpolicies (see Figure 23) are internal rules of the organization which state how special information security-related issues align with the information security policy. This process is based on ISO27001 clauses 8.1, also covers Annex A controls A.5, and controls asking for policies (at least 12 different policies). The actors in this process are ISMS Authority, who coordinates the action and relevant authority (a specialist, group of specialists or relevant manager assigned by ISMS Authority). The starting point is the need for special subpolicy. The need source could be the requirements coming from risk assessment or routine SoA review. The input to the subpolicies are ISO27001, interested party requirements, legal and regulatory requirements and contractual obligations (G0-2). The output of the process is relevant subpolicy(G0-5, G0-11).

BP-4 Security event management Security event management (see Figure 24) is incident management by ISO27001. The experience shows that employees in the organization does not make a difference between the vulnerability or incident or need to change any process or rule. It is suggested to manage mentioned issues in the same place as security events. To assess what is an incident, what a vulnerability or something else, the ISMS Authority should assess it based on risk criteria. Then the ISMS Authority should forward the issue to a relevant channel. This process is based on the ISO27001 clauses: 8.2, 10.1, and Annex A controls under A.16. The starting point of the process is issue of the security event submitted by employee of organization. The inputs to the process are the submitted issue content on the security event template, but also information security policy and subpolicies and risk criteria. The outputs of the process are evidence of security event management process and input to risk assessment and corrective action (G0-11, G0-10).

BP-5 Project management Project management model is adapted project management process (see Figure 7). Internal processes may use the project management process by adding their details. The project management model is basing on the project management workflow model suggested by recognized textbook [6]. Figure 7 shows project management process activities with blue background. ISMS activities are added with yellow background. This process is based on the ISO27001 clauses: 5.1(b), 6.1.3, 6.1.3, 6.2, 7.2, 7.3, 7.4, 8.1, 9.1 and Annex A controls under A.6.1.5 and other internal processes. The starting point of the process is the new project creation. The Actor of the process is Project Manager. To keep the model simple, it does not show the other project members activities implicitly. The input to the project is SoA template or already adapted project SoA template that gives links to relevant documents and requirements of ISMS (G0-2, G0-4). Process has a collapsed subprocess, which is expanded on Figure 26). Subprocess is executed for each issue, which is security related issue and should be linked to SoA project. The outputs of the project are security event reports (if relevant) and evidence of followed process (entry log/history in the ISMS tool) (G0-11, G0-4, G0-9, (G0-5, G0-6, G0-7, G0-8)).

BP-6 Internal audit Internal audit gives feedback about ISMS performance to the relevant manager and top management (G0-3). The described process shows internal audit full process (see Figure 27) – from the audit scope and defining the criteria to follow-up assessment and to corrective actions of nonconformities. The starting point is the receiving date of the internal audit is an audit program. ISMS

Authority starts the process. Other actors in the process are an auditor, auditee and relevant manager. This process is based on the ISO27001 clauses: 6.1.3, 7.2, 7.3, 9.2, 10.1 and Annex A controls under A.18. The input to the process is audit program, audit scope, and criteria, ISO27001 Standard with its requirements and previous nonconformities (G0-2). The output of the internal audit process is audit report, nonconformity reports (if there are any) and evaluation of nonconformity corrective actions (G0-11, G0-8).

BP-7 Compile SoA This process is performed as a next iteration of BP-3. SoA is a required document by external auditors to show which controls organization defines to be relevant from ISO27001 Annex A. This is a part of an audit report. Layer-based ISMS suggests using the SoA as a template for nformation security issues of processes it choose and manage the relevant controls of them. This business process generates the SoA (see Figure 28). The SoA should be reviewed at least a year at least or in the case of significant changes. The trigger of the SoA generation process is the need for (new) SoA. This process is based on the ISO27001 clauses: 6.1.3, 7.5, 5.1, 9. The actors of the process are the ISMS Authority and Management. The input to the process is SoA status board and ISMS scope. The output of the process is the approved SoA. (This SoA can be used as a template to generate information security issues in the other projects.)(G0-11, G0-9, G0-4)

BP-8 Management review Management review is the commitment of top management to evaluate the performance of ISMS and to ensure its adequacy and effectiveness (G0-1). The process (see Figure 29) is basing on ISO27001 clauses 9.3 and 7.4. The actors of the process are the ISMS Authority and Management (i.e. Top Management). The starting point is the upcoming external audit. Management review should be done before the audit. The input to the management review is previous management review results, Interested parties requirements (changes), audit results, monitoring and measurement results, nonconformities, corrective actions, SoA, risk treatment plan (G0-11). The output of the process is management review results, that could contain IS policy, confirmed new SoA version, new IS objectives (G0-11, G0-10).

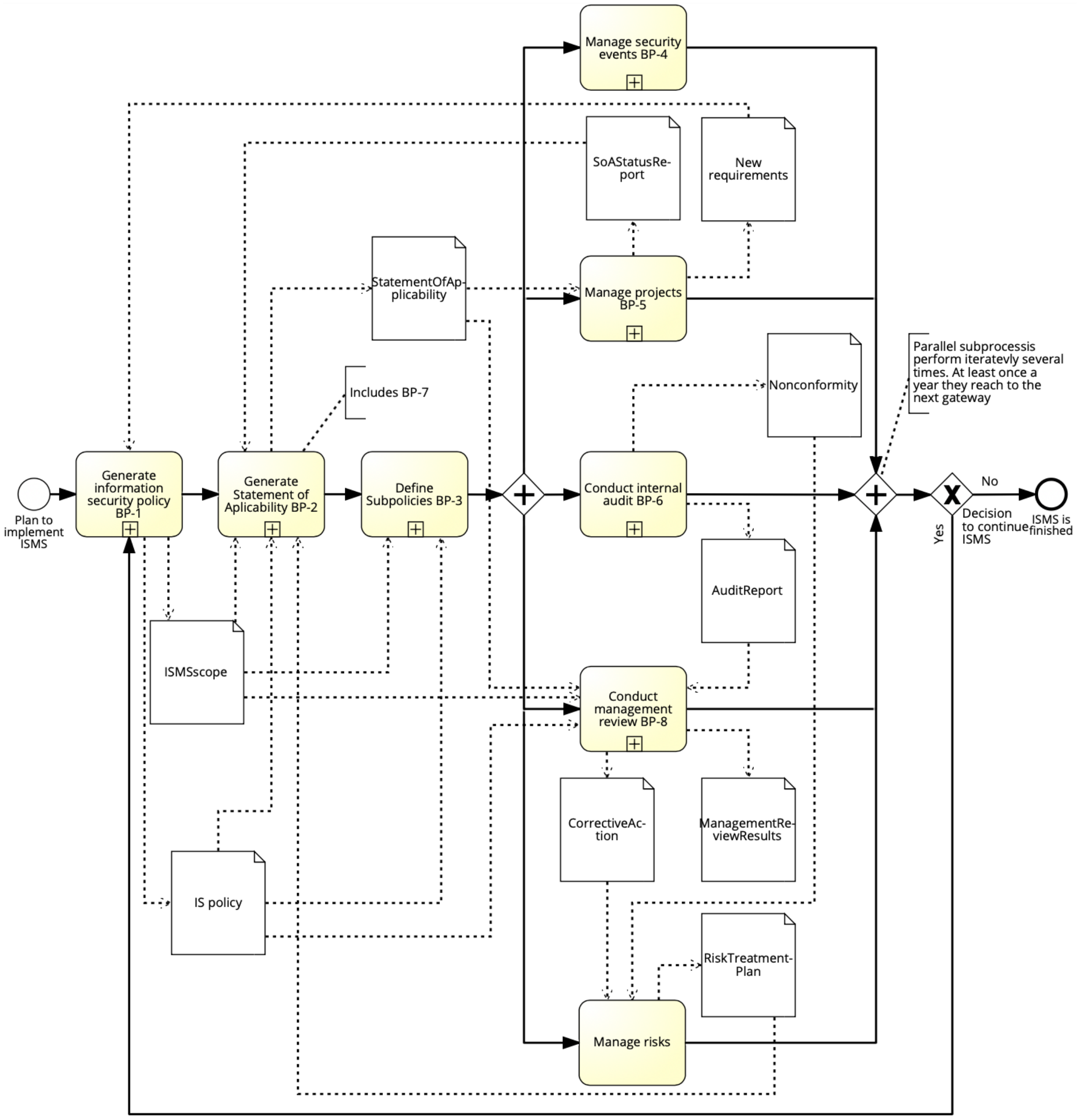

Manage security events BP-4
SoAStatusReport
New requirements
StatementOfApplicability
Manage projects BP-5
Includes BP-7
Nonconformity
Parallel subprocessis perform iterativly several times. At least once a year they reach to the next gateway
Plan to implement ISMS
Generate information security policy BP-1
Generate Statement of Aplicability BP-2
Define Subpolicies BP-3
Conduct internal audit BP-6
No
Yes
Decision to continue ISMS
ISMS is finished
AuditReport
ISMSscope
Conduct management review BP-8
CorrectiveAction
ManagementReviewResults
IS policy
RiskTreatmentPlan
Manage risks

Figure 20. BP-G ISMS general business model.

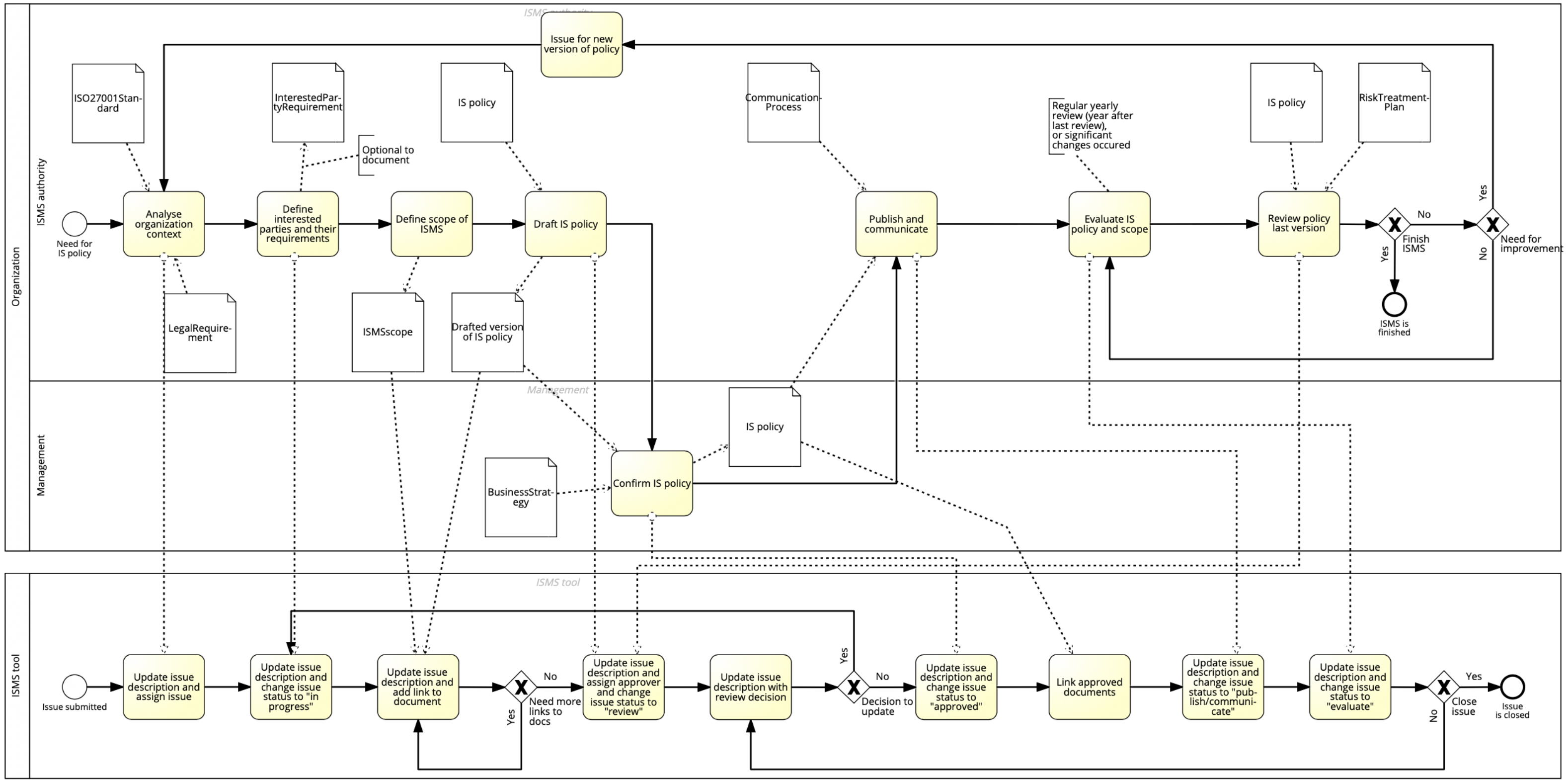

Organization
ISMS authority
Management
ISMS tool
Need for IS policy
Analyse organization context
ISO27001Standard
LegalRequirement
Define interested parties and their requirements
InterestedPartyRequirement
Optional to document
Define scope of ISMS
ISMSscope
Draft IS policy
IS policy
Drafted version of IS policy
Issue for new version of policy
Publish and communicate
Communication-Process
Evaluate IS policy and scope
Regular yearly review (year after last review), or significant changes occured
Review policy last version
IS policy
RiskTreatment-Plan
Finish ISMS
Yes
No
ISMS is finished
Need for improvement
Yes
No
BusinessStrategy
Confirm IS policy
IS policy
Issue submitted
Update issue description and assign issue
Update issue description and change issue status to "in progress"
Update issue description and add link to document
Need more links to docs
Yes
No
Update issue description and assign approver and change issue status to "review"
Update issue description with review decision
Decision to update
Yes
No
Update issue description and change issue status to "approved"
Link approved documents
Update issue description and change issue status to "publish/communicate"
Update issue description and change issue status to "evaluate"
Close issue
Yes
No
Issue is closed

Figure 21. BP-1 Define information security policy

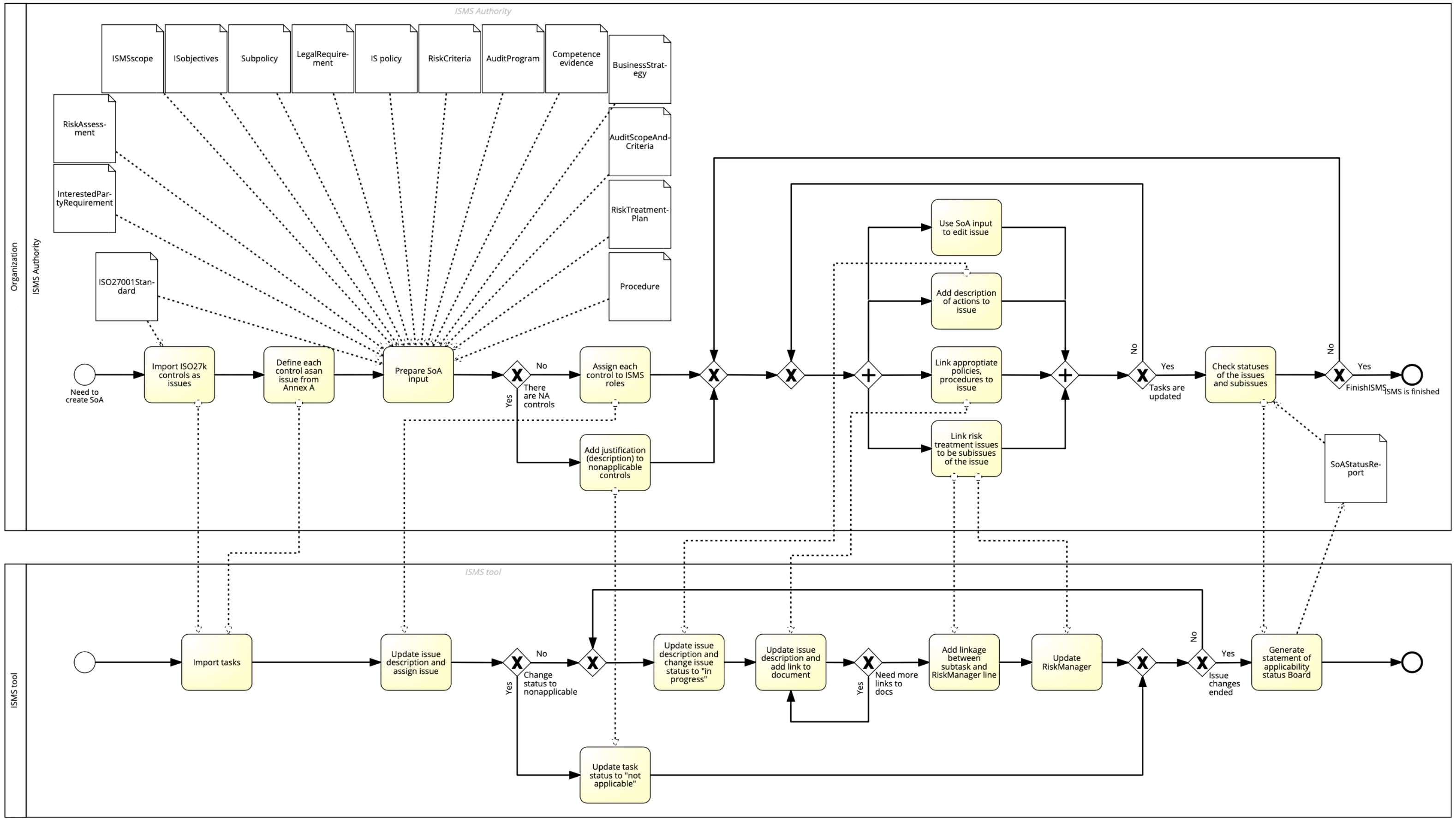

Organization
ISMS Authority
ISMS Authority
ISMSscope
ISobjectives
Subpolicy
LegalRequire-ment
IS policy
RiskCriteria
AuditProgram
Competence evidence
BusinessStrat-egy
RiskAssess-ment
InterestedPar-tyRequirement
AuditScopeAnd-Criteria
RiskTreatment-Plan
ISO27001Stan-dard
Procedure
Need to create SoA
Import ISO27k controls as issues
Define each control asan issue from Annex A
Prepare SoA input
No
Yes
There are NA controls
Assign each control to ISMS roles
Add justification (description) to nonapplicable controls
Use SoA input to edit issue
Add description of actions to issue
Link appropriate policies, procedures to issue
Link risk treatment issues to be subissues of the issue
No
Yes
Tasks are updated
Check statuses of the issues and subissues
No
Yes
FinishISMS
ISMS is finished
SoAStatusRe-port
ISMS tool
ISMS tool
Import tasks
Update issue description and assign issue
No
Yes
Change status to nonapplicable
Update task status to "not applicable"
Update issue description and change issue status to "in progress"
Update issue description and add link to document
Yes
Need more links to docs
Add linkage between subtask and RiskManager line
Update RiskManager
No
Yes
Issue changes ended
Generate statement of applicability status Board

Figure 22. BP-2 Compile SoA first version

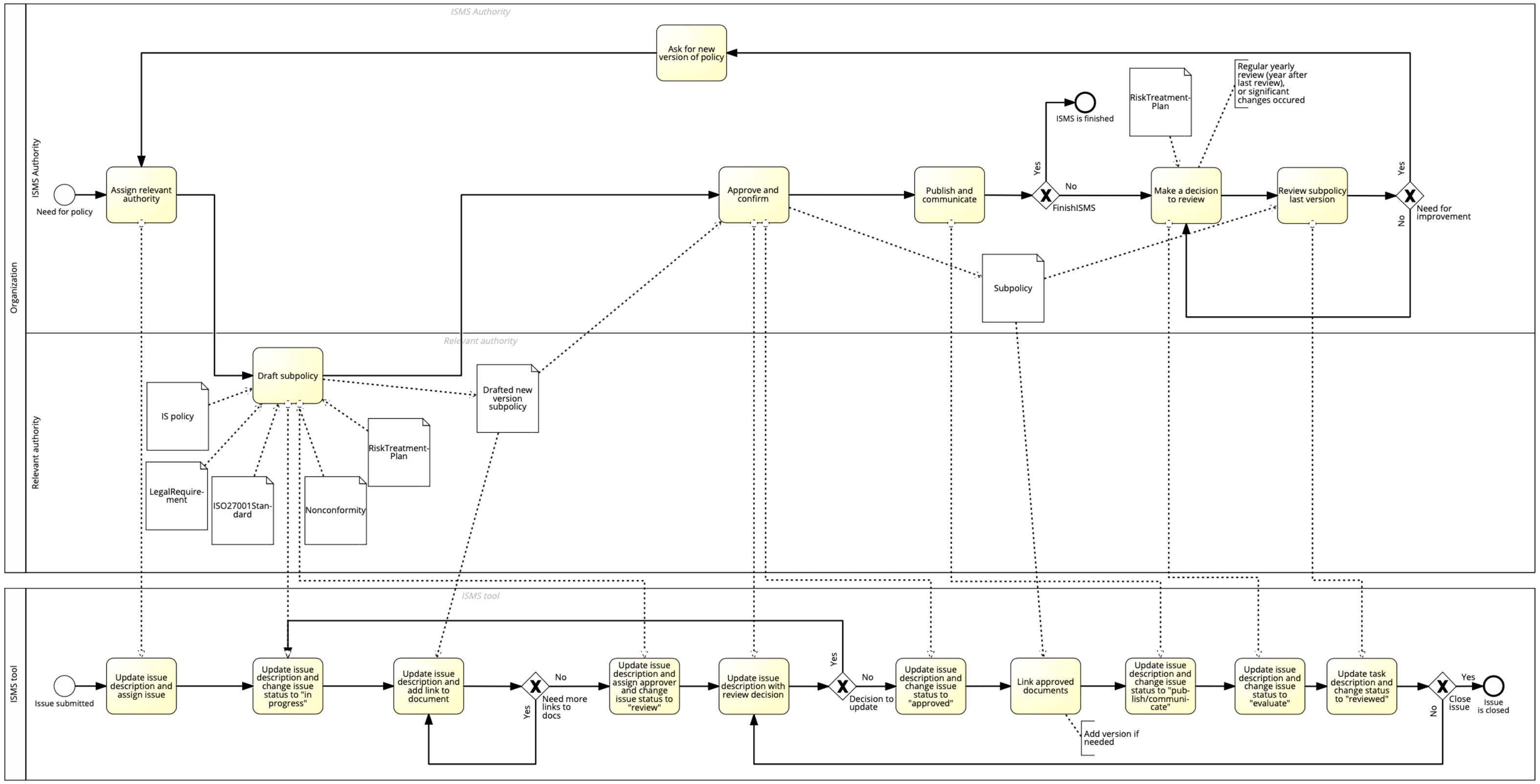

Organization
ISMS Authority
ISMS Authority
Need for policy
Assign relevant authority
Ask for new version of policy
Approve and confirm
Publish and communicate
Yes
No
FinishISMS
ISMS is finished
RiskTreatment-Plan
Regular yearly review (year after last review), or significant changes occured
Make a decision to review
Review subpolicy last version
Yes
No
Need for improvement
Subpolicy
Relevant authority
Relevant authority
Draft subpolicy
IS policy
LegalRequire-ment
ISO27001Stan-dard
Nonconformity
RiskTreatment-Plan
Drafted new version subpolicy
ISMS tool
ISMS tool
Issue submitted
Update issue description and assign issue
Update issue description and change issue status to "in progress"
Update issue description and add link to document
No
Yes
Need more links to docs
Update issue description and assign approver and change issue status to "review"
Update issue description with review decision
Yes
No
Decision to update
Update issue description and change issue status to "approved"
Link approved documents
Add version if needed
Update issue description and change issue status to "pub-lish/communi-cate"
Update issue description and change issue status to "evaluate"
Update task description and change status to "reviewed"
Yes
No
Close issue
Issue is closed

Figure 23. BP-3 Defining subpolicy

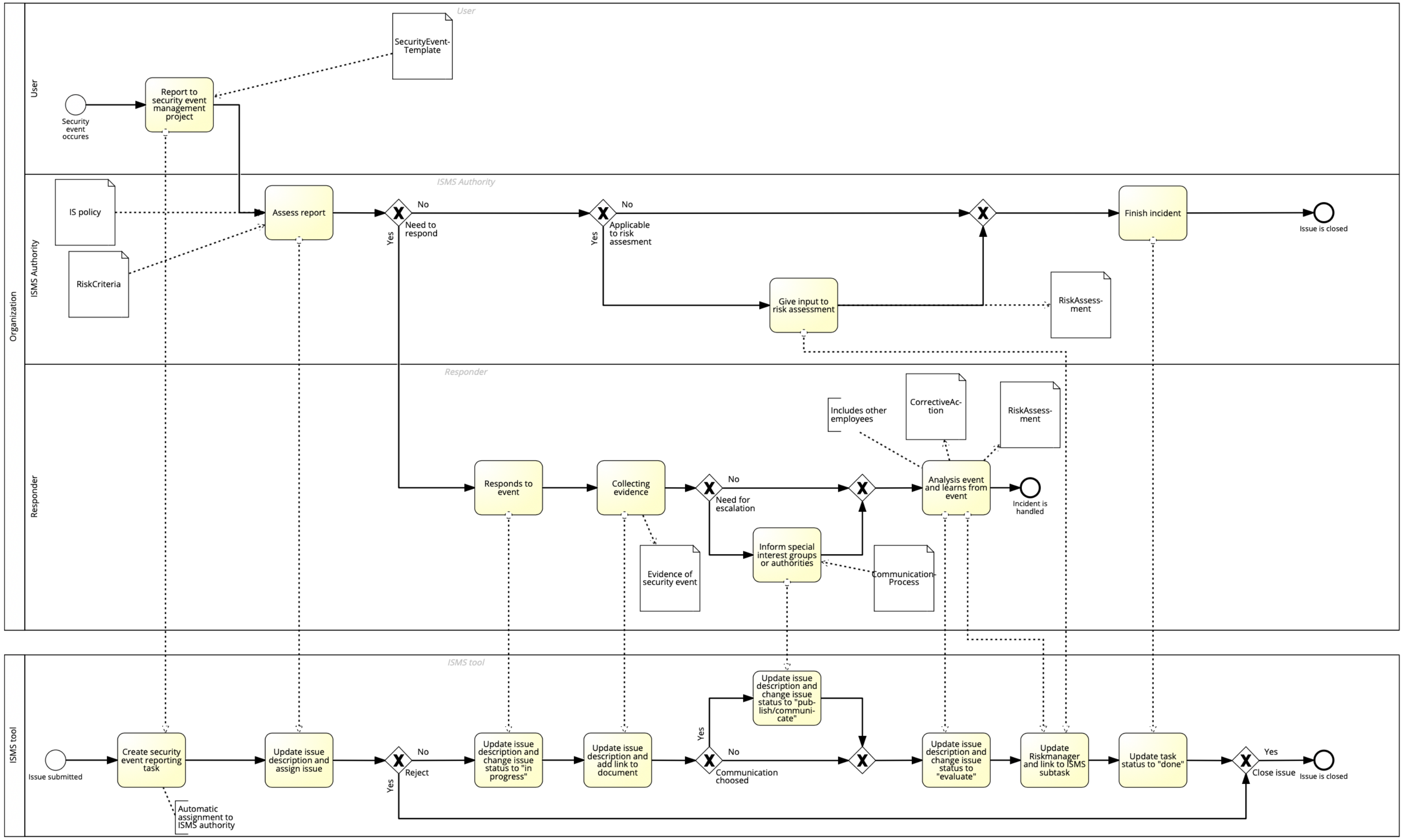

Organization
User
ISMS Authority
Responder
ISMS tool
Security event occures
Report to security event management project
SecurityEvent-Template
IS policy
RiskCriteria
Assess report
No
Yes
Need to respond
No
Yes
Applicable to risk assesment
Give input to risk assessment
RiskAssess-ment
Finish incident
Issue is closed
Responds to event
Collecting evidence
Evidence of security event
No
Need for escalation
Inform special interest groups or authorities
Communication-Process
Includes other employees
CorrectiveAc-tion
RiskAssess-ment
Analysis event and learns from event
Incident is handled
Issue submitted
Create security event reporting task
Automatic assignment to ISMS authority
Update issue description and assign issue
No
Yes
Reject
Update issue description and change issue status to "in progress"
Update issue description and add link to document
Yes
No
Communication choosed
Update issue description and change issue status to "pub-lish/communi-cate"
Update issue description and change issue status to "evaluate"
Update Riskmanager and link to ISMS subtask
Update task status to "done"
Yes
Close issue
Issue is closed

Figure 24. BP-4 Security event management

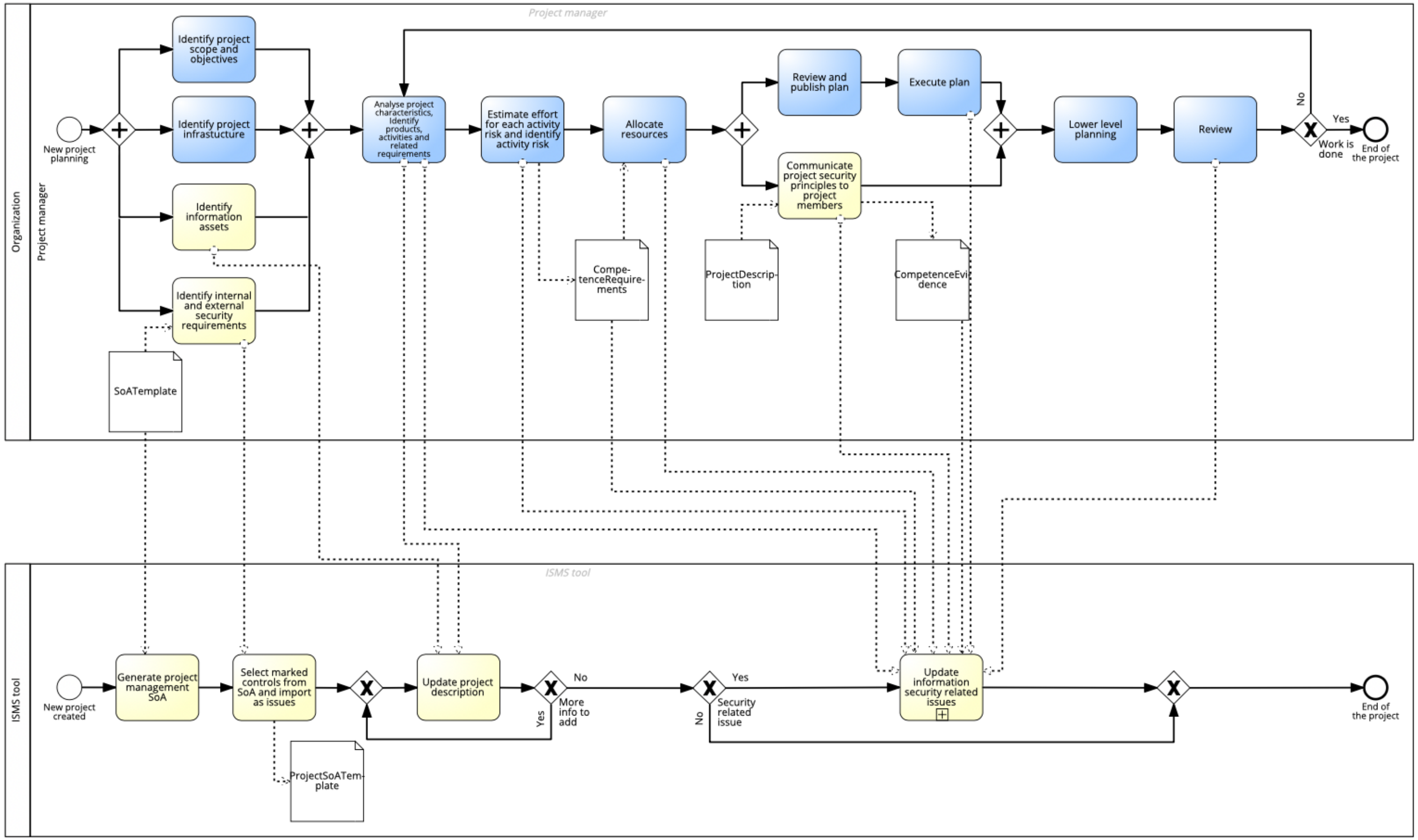

Organization
Project manager
Project manager
New project planning
Identify project scope and objectives
Identify project infrastucture
Identify information assets
Identify internal and external security requirements
SoATemplate
Analyse project characteristics, Identify products, activities and related requirements
Estimate effort for each activity risk and identify activity risk
Compe-tenceRequire-ments
Allocate resources
Review and publish plan
Execute plan
Communicate project security principles to project members
ProjectDescrip-tion
CompetenceEvi-dence
Lower level planning
Review
No
Yes
Work is done
End of the project
ISMS tool
ISMS tool
New project created
Generate project management SoA
Select marked controls from SoA and import as issues
ProjectSoATem-plate
Update project description
No
Yes
More info to add
Yes
No
Security related issue
Update information security related issues
End of the project

Figure 25. BP-5 Project management

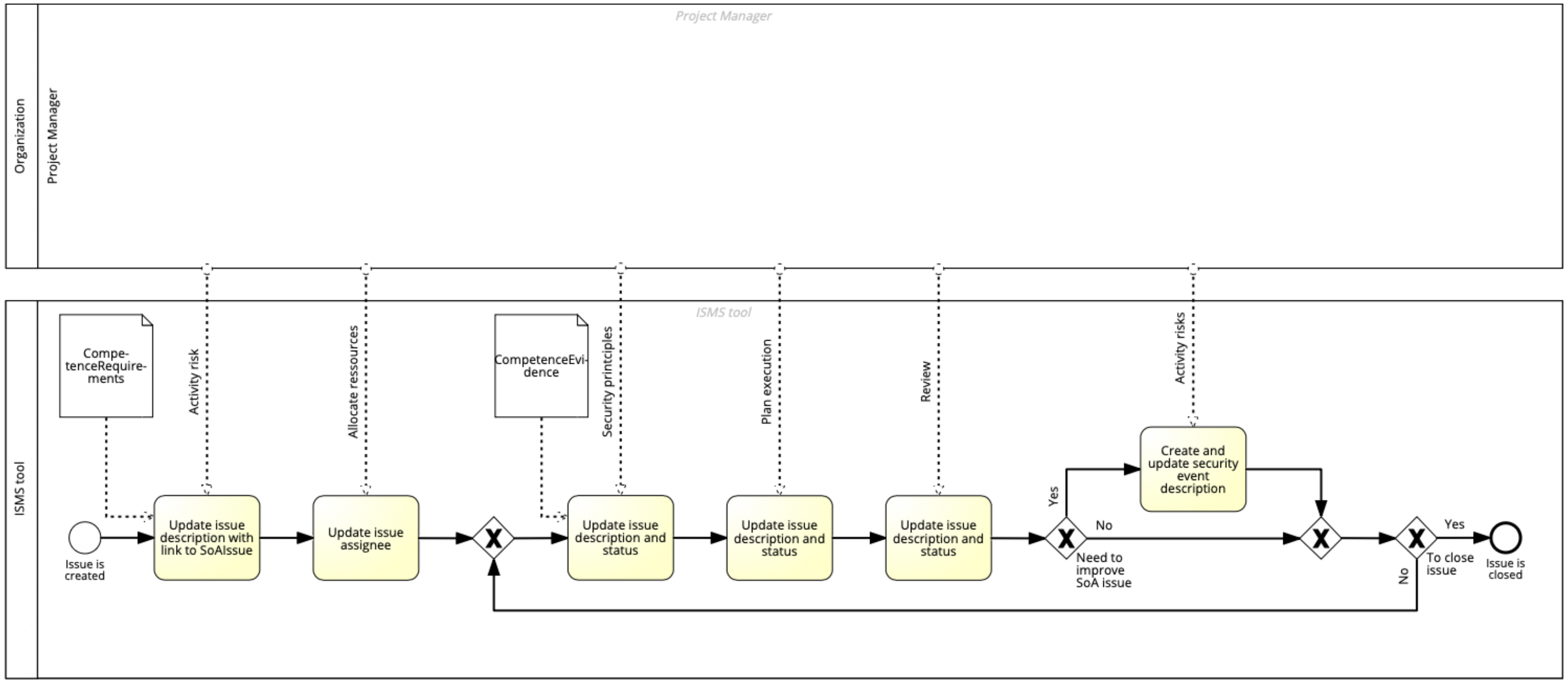


Figure 26. BP-5a Project management subprocess: Update information security related issues

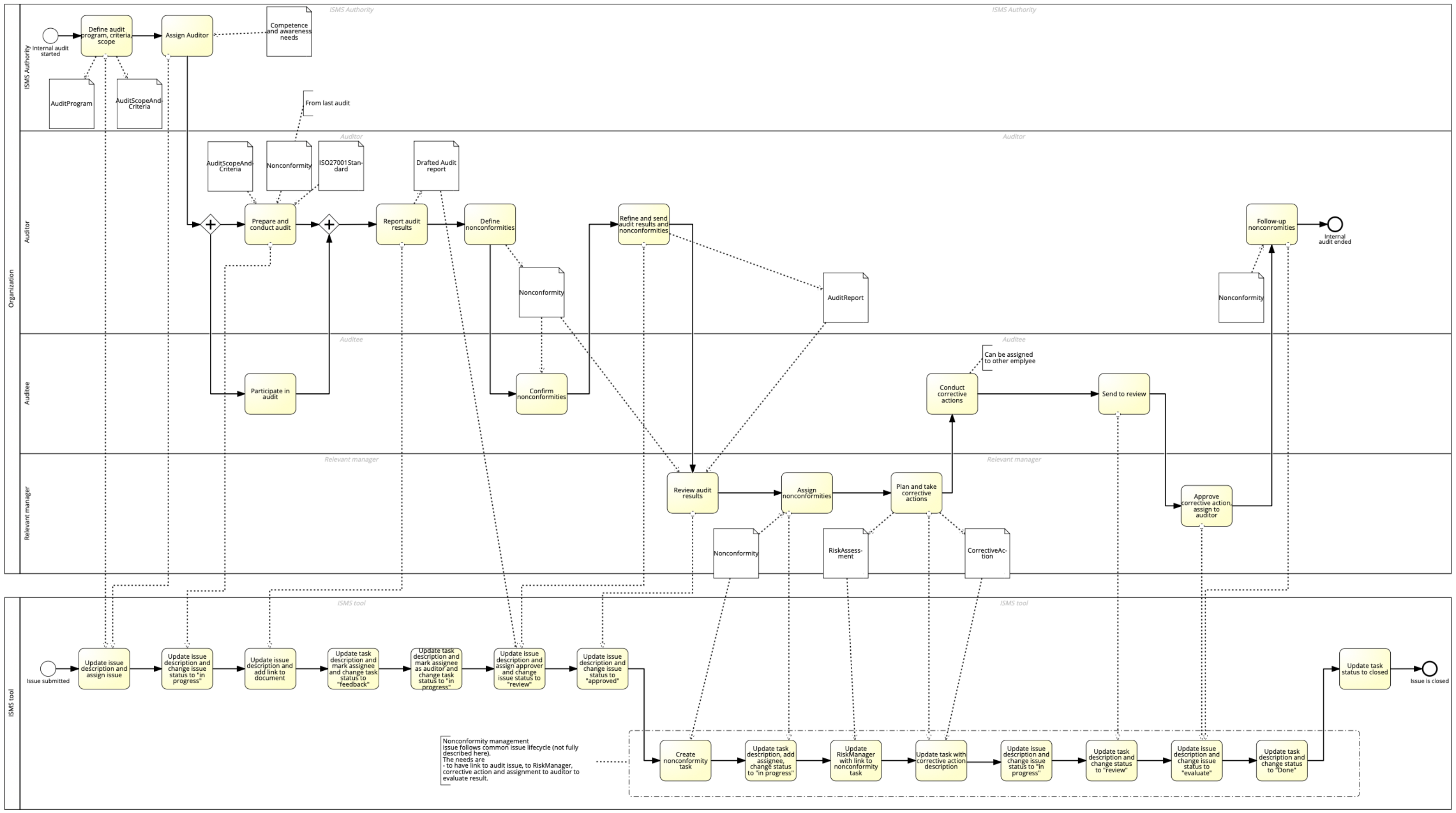
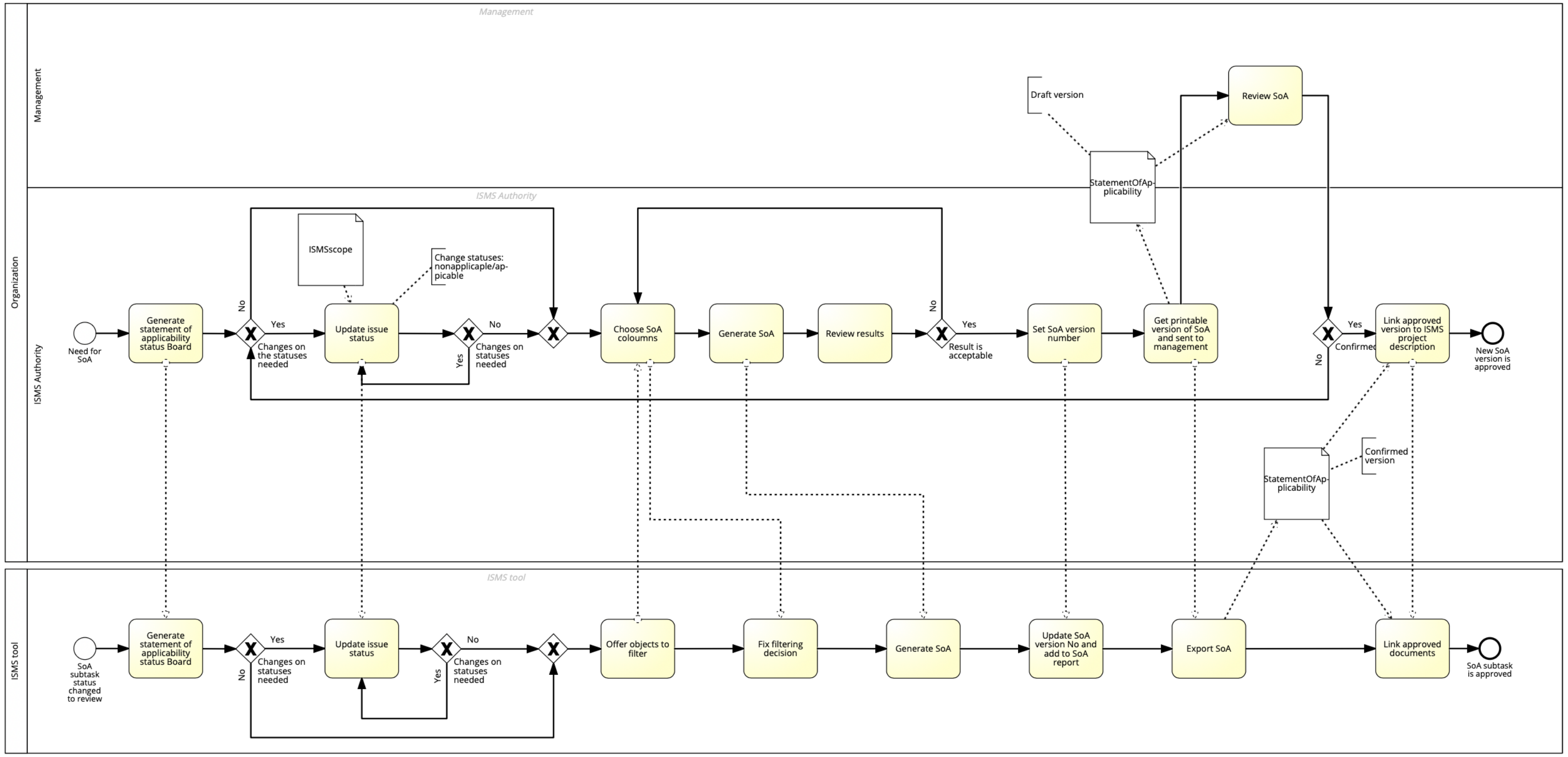
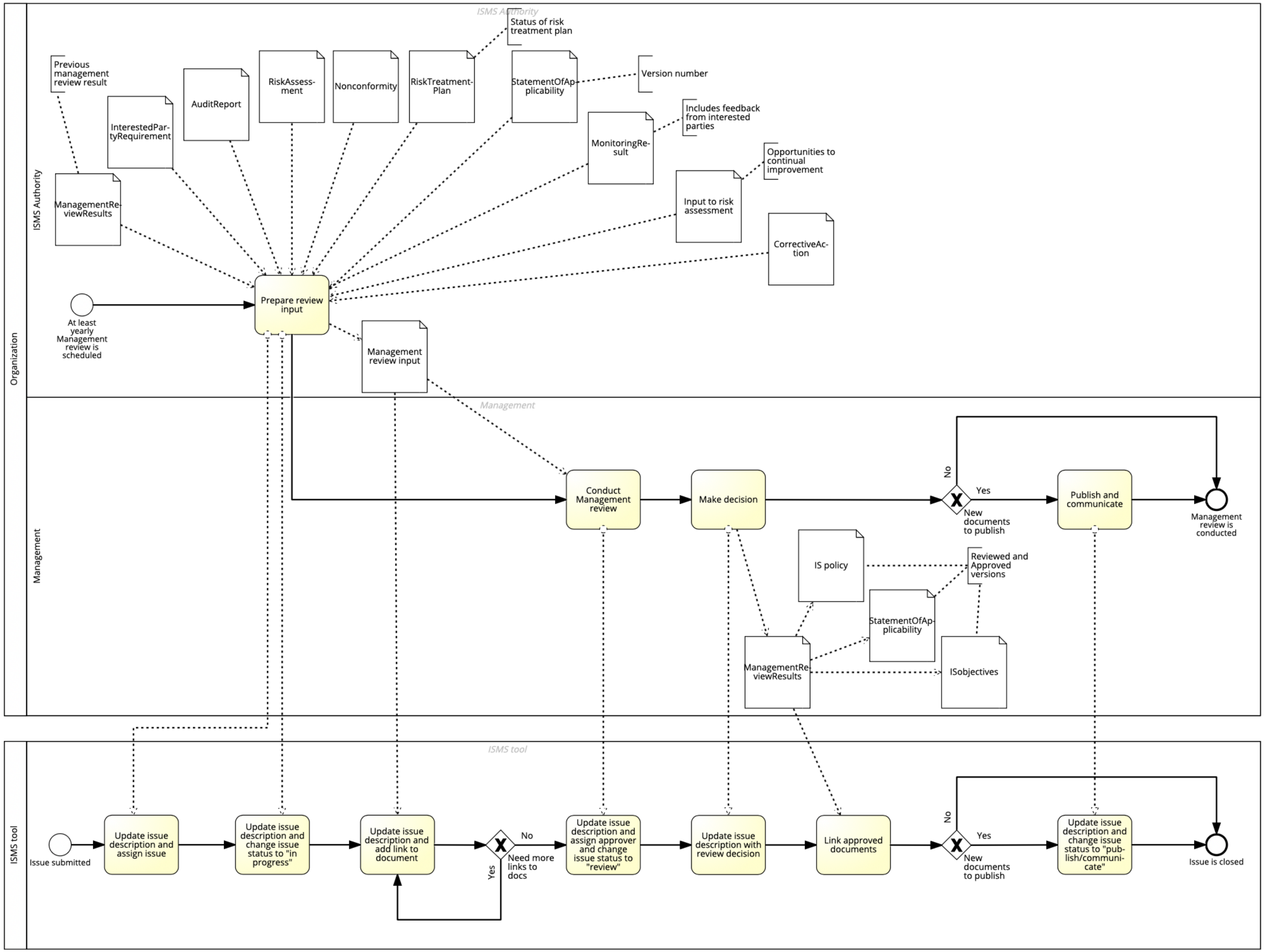

Organization
ISMS Authority
Internal audit started
Define audit program, criteria, scope
AuditProgram
AuditScopeAndCriteria
Assign Auditor
Competence and awareness needs
From last audit
Auditor
AuditScopeAndCriteria
Nonconformity
ISO27001Standard
Prepare and conduct audit
Report audit results
Drafted Audit report
Define nonconformities
Nonconformity
Refine and send audit results and nonconformities
AuditReport
Follow-up nonconromities
Nonconformity
Internal audit ended
Auditee
Participate in audit
Confirm nonconformities
Can be assigned to other emplyee
Conduct corrective actions
Send to review
Relevant manager
Review audit results
Assign nonconformities
Plan and take corrective actions
Nonconformity
RiskAssessment
CorrectiveAction
Approve corrective action, assign to auditor
ISMS tool
Issue submitted
Update issue description and assign issue
Update issue description and change issue status to "in progress"
Update issue description and add link to document
Update task description and mark assignee and change task status to "feedback"
Update task description and mark assignee as auditor and change task status to "in progress"
Update issue description and assign approver and change issue status to "review"
Update issue description and change issue status to "approved"
Nonconformity management issue follows common issue lifecycle (not fully described here).
The needs are
- to have link to audit issue, to RiskManager, corrective action and assignment to auditor to evaluate result.
Create nonconformity task
Update task description, add assignee, change status to "in progress"
Update RiskManager with link to nonconformity task
Update task with corrective action description
Update issue description and change issue status to "in progress"
Update task description and change status to "review"
Update issue description and change issue status to "evaluate"
Update task description and change status to "Done"
Update task status to closed
Issue is closed

Figure 27. BP-6 Internal audit



Organization
Management
ISMS Authority
ISMS tool
Need for SoA
Generate statement of applicability status Board
No
Yes
Changes on the statuses needed
Update issue status
ISMSscope
Change statuses: nonapplicaple/ap-picable
No
Yes
Changes on statuses needed
Choose SoA coloumns
Generate SoA
Review results
No
Yes
Result is acceptable
Set SoA version number
Get printable version of SoA and sent to management
Draft version
StatementOfAp-plicability
Review SoA
No
Yes
Confirmed
Link approved version to ISMS project description
New SoA version is approved
StatementOfAp-plicability
Confirmed version
SoA subtask status changed to review
Generate statement of applicability status Board
Yes
No
Changes on statuses needed
Update issue status
No
Yes
Changes on statuses needed
Offer objects to filter
Fix filtering decision
Generate SoA
Update SoA version No and add to SoA report
Export SoA
Link approved documents
SoA subtask is approved

Figure 28. BP-7 Compile SoA



Organization
ISMS Authority
ISMS Authority
Previous management review result
ManagementReviewResults
InterestedPartyRequirement
AuditReport
RiskAssessment
Nonconformity
RiskTreatmentPlan
Status of risk treatment plan
StatementOfApplicability
Version number
MonitoringResult
Includes feedback from interested parties
Input to risk assessment
Opportunities to continual improvement
CorrectiveAction
At least yearly Management review is scheduled
Prepare review input
Management review input
Management
Management
Conduct Management review
Make decision
No
Yes
New documents to publish
Publish and communicate
Management review is conducted
IS policy
Reviewed and Approved versions
StatementOfApplicability
ManagementReviewResults
ISobjectives
ISMS tool
ISMS tool
Issue submitted
Update issue description and assign issue
Update issue description and change issue status to "in progress"
Update issue description and add link to document
No
Yes
Need more links to docs
Update issue description and assign approver and change issue status to "review"
Update issue description with review decision
Link approved documents
No
Yes
New documents to publish
Update issue description and change issue status to "publish/communicate"
Issue is closed

Figure 29. BP-8 Management review

C.5 ISMS tool functionality

Based on the business process analysis (see Section C.4), each modeled activity in the ISMS tool pool was analyzed separately. The purpose was to find similarities and differences and the need to have the use case(s). The result was ISMS tool use case diagram that shows the needed system functionality of layer-based ISMS tool (see Figure 30).

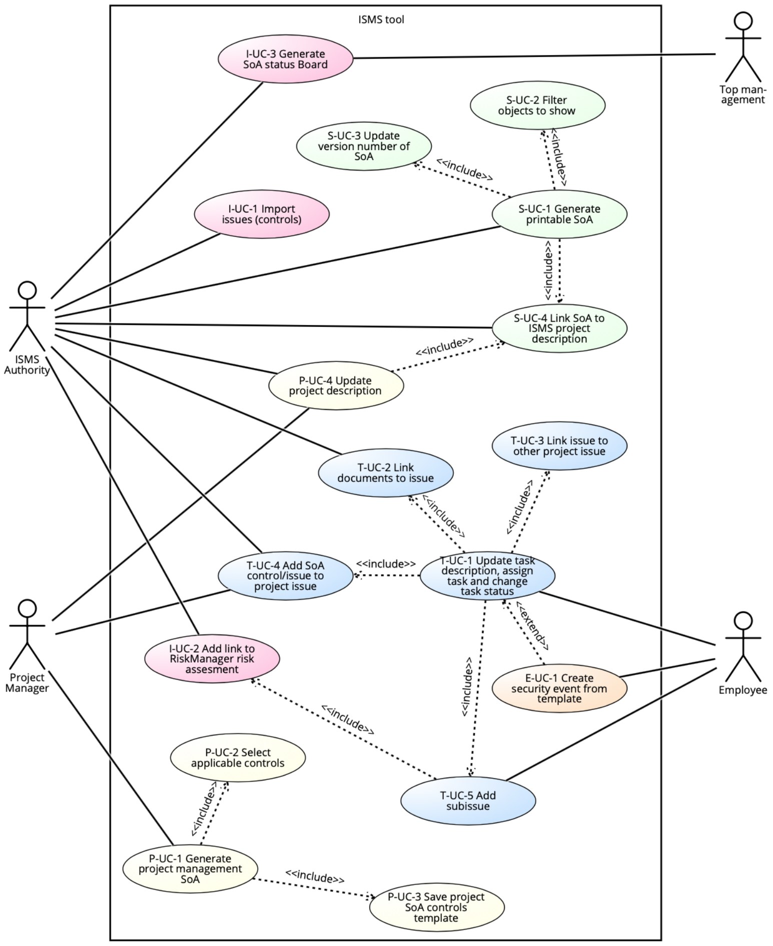

ISMS tool
I-UC-3 Generate SoA status Board
Top management
S-UC-2 Filter objects to show
S-UC-3 Update version number of SoA
<<include>>
<<include>>
I-UC-1 Import issues (controls)
S-UC-1 Generate printable SoA
<<include>>
S-UC-4 Link SoA to ISMS project description
ISMS Authority
<<include>>
P-UC-4 Update project description
T-UC-3 Link issue to other project issue
T-UC-2 Link documents to issue
<<include>>
<<include>>
T-UC-4 Add SoA control/issue to project issue
<<include>>
T-UC-1 Update task description, assign task and change task status
<<extend>>
Project Manager
I-UC-2 Add link to RiskManager risk assesment
<<include>>
E-UC-1 Create security event from template
Employee
<<include>>
P-UC-2 Select applicable controls
T-UC-5 Add subissue
<<include>>
P-UC-1 Generate project management SoA
<<include>>
P-UC-3 Save project SoA controls template

Figure 30. ISMS tool functionality

The use case diagram is used for completing ISMS tool functionality descriptions (Section C.6).

Use cases have related to human Actors who participate in the use case as ISMS tool users. Actors can have several roles.

Employee organization member, who can be in the same time in the roles that are described in the business process models, for example, Project Manager, Internal Auditor, Auditee, Relevant manager, Responder, ISMS Authority.

ISMS Authority organization member, who is the project manager of ISMS project (or process manager of ISMS process - depends on how organization names it)

Top management - organization member who reviews of ISMS performance

Project Manager organization member who manages projects, could also be organizational process manager

As shown on Figure 30 there is identified 17 preliminary use cases. Use cases are divided into modules by their usage objective: manage issues (T-group), manage security events/incidents (E-group), manage ISMS project (I-group), manage projects and processes (P-group), manage statement of applicability (S-group). The Figure 31 illustrates the use cases dividing into modules.

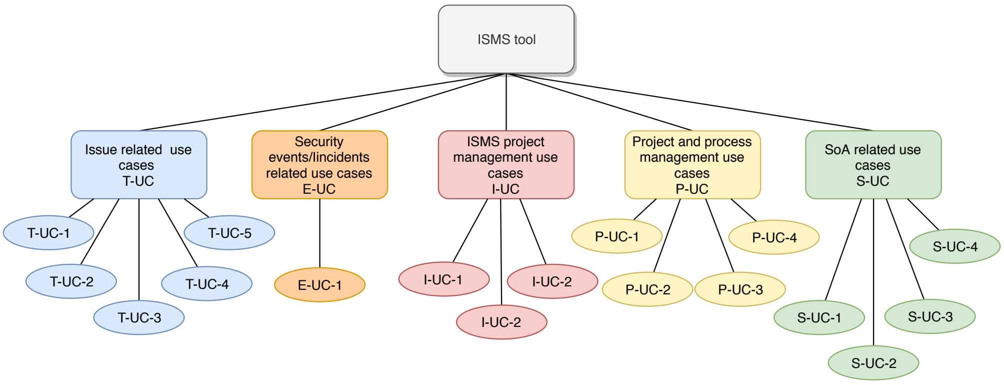


Figure 31. Modules of the ISMS tool use cases.

Use cases have natural language descriptions in the Section C.6. Links to the concrete use case description is given in the next list.

Issue related use cases Use cases which describe the functons of business processes for issue management (marked on the Figures 30 and 31 as blue):

- T-UC-1 Update issue description, assign issue and change issue status (see on Table 5)

- T-UC-2 Add to issue a document link (see on Table 6)
- T-UC-3 Link issue to other project issues (see on Table 7)
- T-UC-4 Add link to project SoA control (see on Table 8)
- T-UC-5 Add subissue(see on Table 9)

Security Events/incidents related use cases Use cases for security event management,(including vulnerability and incident management) (marked on the Figures 30 and 31 as orange):

- E-UC-1 Create security event from template (see on Table 10)

ISMS project management related use cases Use cases that are specific only for ISMS project management (marked on the Figures 30 and 31 as pink):

- I-UC-1 Import issues (controls) (see on Table 11)
- I-UC-2 Add link to Risk Manager risk assessment (see on Table 12)
- I-UC-3 Generate SoA status Board (see on Table 13)

Project or process management related use cases Use cases for projects handled in the scope of ISMS (marked on the Figures 30 and 31 as yellow):

- P-UC-1 Generate project management SoA (see on Table 14)
- P-UC-2 Select applicable controls (see on Table 15)
- P-UC-3 Save project SoA controls template (see on Table 16)
- P-UC-4 Update project description (see on Table 17)

Statement of applicability related use cases Use cases that are specific for statement of applicability management. These use cases are not relevant only for the ISMS project but also in other projects which belong to the scope of ISMS (use cases are marked on the Figures 30 and 31 as green):

- S-UC-1 Generate printable SoA (see on Table 18)
- S-UC-2 Filter objects to show (see on Table 19)
- S-UC-3 Update version number of SoA (see on Table 20)
- S-UC-4 Link SoA to ISMS project description (see on Table 21)

C.6 ISMS tool functions

The Section contains 17 use case description for ISMS tool in tabled form.

Table 5. Use case T-UC-1

No.	Section	Content
1.	Identifier	T-UC-1
2.	Name	Update issue description, assign issue and change issue status
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	High
6.	Criticality	To trace controls, to keep user to follow workflow
7.	Source	BP-1 Define information security policy, BP-3 Defining subpolicy, BP-6 Internal audit, BP-8 Management review
8.	Short Description	User opens issue and updates issue description, assignee and status.
9.	Goal(s)	G0-11, G0-10, G0-4, G0-09
10.	Actor(s)	Employee
11.	Precondition	Issue workflow is defined. Issue is created.
12.	Postcondition	Issue has description, assignee and/or status is updated.
13.	Main scenario	1. System displays list of issues. 2. User opens the issue. 3. System displays the information of issue. 4. User starts editing the information of issue. 5. User writes a comment(optional). 6. User changes an assignee (optional). 7. User changes the issue status by following the defined issue workflow (optional). 8. System updates the information of issue. 9. System logs activities. 10. System notifies issue assignee about the update of issue.
14.	Alternative scenario	Steps 5.-7. are optional. User can cancel editing in any step.
15.	Related use cases	extended by Use case T-UC-2, Use case T-UC-3 , Use case T-UC-4 , Use case T-UC-5 , Use case E-UC-1

Table 6. Use case T-UC-2

No.	Section	Content
1.	Identifier	T-UC-2
2.	Name	Add to issue a document link
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	Medium
6.	Criticality	To make info available there where it is needed
7.	Source	BP-1 Define information security policy, BP-2 Compile SoA first version, BP-3 Defining subpolicy, BP-4 Security event management, BP-5 Project management, BP-6 Internal audit, BP-8 Management review
8.	Short Description	User has link to a document (link to Confluence) and adds this link to the special field of the issue so that the link will be a part of the issue info.
9.	Goal(s)	G0-11, G0-10, G0-4, GO-7
10.	Actor(s)	Employee
11.	Precondition	Issue is created
12.	Postcondition	The link of the document added to the issue is accessible to the users.
13.	Main scenario	1. User opens the issue to edit. 2. User selects a document link to add to the issue on special field in the issue information. 3. System updates the issue info with a document link.
14.	Alternative scenario	2a. User adds document link to the issue description. Proceed to step 3.
15.	Related use cases	extension of Use case T-UC-1

Table 7. Use case T-UC-3

No.	Section	Content
1.	Identifier	T-UC-3
2.	Name	Link issue to the other project issue
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	Medium
6.	Criticality	Traceability
7.	Source	BP-4 Security event management
8.	Short Description	User links issue to be the ISMS project subissue.
9.	Goal(s)	G0-11, G0-10, G0-4, G0-09
10.	Actor(s)	ISMS authority or Project Manager
11.	Precondition	The issue is created and open to edit.
12.	Postcondition	The issue is linked to the ISMS project issue.
13.	Main scenario	1. User chooses the project to link the issue. 2. System provides the linkable projects. 3. User selects the project. 4. User selects the issue. 5. System displays selected issue summary. 6. User selects the issue to add link between issues. 7. System updates the issues info with added link.
14.	Alternative scenario	6a. User select an other issue to read the summary of issue. Proceed step 5.
15.	Related use cases	extension of Use case T-UC-1

Table 8. Use case T-UC-4

No.	Section	Content
1.	Identifier	T-UC-4
2.	Name	Link issue to project-SoA control
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	Medium
6.	Criticality	Traceability
7.	Source	BP-5 Project management
8.	Short Description	User links ordinary issue to be subissue of issue, which is project-SoA issue
9.	Goal(s)	G0-11, G0-4, G0-7
10.	Actor(s)	Employee
11.	Precondition	SoA controls are created to be the project issues. User edits the issue, what isn't linked to SoA controls.
12.	Postcondition	The issue is linked to be the project-SoA control (issue) subissue.
13.	Main scenario	1. User selects linkable project-SoA issue . 2. System update the linking info. 3. System displays link.
14.	Alternative scenario	1a. User selects several issues to link. Proceed to the step 2. 4. User repeats from the step 1.
15.	Related use cases	extension of Use case T-UC-1, precondition Use case I-UC-1

Table 9. Use case T-UC-5

No.	Section	Content
1.	Identifier	T-UC-5
2.	Name	T-UC-5 Add subissue
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	High
6.	Criticality	Possibility to use different issue types in the project
7.	Source	BP-1 Define information security policy, BP-2 Compile SoA first version, BP-3 Defining subpolicy, BP-6 Internal audit, BP-8 Management review
8.	Short Description	User creates the issue and submits it as the subissue to choosed parent issue.
9.	Goal(s)	G0-11, G0-10, G0-4, G0-09, G0-7
10.	Actor(s)	Employee
11.	Precondition	Use case T-UC-1
12.	Postcondition	The issue is findable as a subissue of other issue(s).
13.	Main scenario	1. System provides the list of issues for selection. 2. User selects and fixes a parent issue to his issue. 3. System updates the issue info
14.	Alternative scenario	-
15.	Related use cases	extension of Use case T-UC-1

Table 10. Use case E-UC-1

No.	Section	Content
1.	Identifier	E-UC-1
2.	Name	Create security event from template
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	Medium
6.	Criticality	To get from user an adequate info to assess the criticality of the submitted issue and to respond effectively to that.
7.	Source	BP-5 Project management
8.	Short Description	User creates a security event issue from the template.
9.	Goal(s)	G0-11, G0-10
10.	Actor(s)	Employee
11.	Precondition	Issue template is created
12.	Postcondition	System provides to use a template, when user wants to report of any security event or vulnerability or incident or other observation.
13.	Main scenario	1. User opens security event reporting project. 2. User selects security event reporting issue template to fulfill. 3. User submits filled report. 4. System displays submitted issue info to user. 5. System sends a notification of the submitted issue to the defind responder/ISMS Authority
14.	Alternative scenario	2a. User does not choose template. 3a. User describes his observation in written form of issue content. Proceed to step 3.
15.	Related use cases	extension of Use case T-UC-1

Table 11. Use case I-UC-1

No.	Section	Content
1.	Identifier	I-UC-1
2.	Name	Import issues (controls)
3.	Author	Mari Seeba
4.	Change history	25.03.2019
5.	Priority	High
6.	Criticality	Starting point of SoA
7.	Source	BP-2 Compile SoA first version
8.	Short Description	User prepares (or uses already prepared) input (for example, CSV) file to import ISO27001 Annex A and ISO27001 main part controls into ISMS project.
9.	Goal(s)	G0-7, G0-2
10.	Actor(s)	ISMS Authority
11.	Precondition	ISMS project is created
12.	Postcondition	ISMS project has imported list of issues of ISMS controls
13.	Main scenario	1. User prepares the input file with ISO27001 main part controls and Annex A controls 2. User imports file to the system. 3. System creates issues. 4. User details the issues custom field "Relevance" to be "applicable" or "nonapplicable" 5. System saves the field to the issues 6. User details the issue and subissues workflow to "toDo" –>"in progress" –> "in review" –>"approved" –> "to communicate" –>"evaluate" –> "Done" with backward ability 7. System saves the workflow to subissues.
14.	Alternative scenario	1.a User enters the issues manually into the system. Proceed with step 3. Begin after 6. 6.a User adds custom statuses to the workflow. Proceed with step 7.
15.	Related use cases	Precondition to Use case I-UC-3, Use case P-UC-1

Table 12. Use case I-UC-2

No.	Section	Content
1.	Identifier	I-UC-2
2.	Name	Add link to RiskManager risk assesment
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	High
6.	Criticality	Tracing risk is mandatory for ISMS
7.	Source	BP-2 Compile SoA first version, BP-4 Security event management
8.	Short Description	ISMS Authority links the Security event issue to the Risk Manager and risk treatment and the verification issue to be the ISMS project subissue. NOTE: *this use case is closely related with Jira adds-on RiskManager developed by SoftComply.*
9.	Goal(s)	G0-11, G0-7
10.	Actor(s)	ISMS Authority
11.	Precondition	ISMS Authority gets a notification of the submitted security event, which needs to manage as a risk of ISMS.
12.	Postcondition	Traceability from the submitted Security event report to the evaluation.
13.	Main scenario	1. User opens the Risk Manager. 2. System shows the status board of Risk Manager. 3. User adds the risk line into the Risk Manager (the line includes the Security event issue info (link)). 4. System saves Risk Manager changes. 5. User adds the subissue to the ISMS project to treat risk. 6. System saves the subissue. 7. User complements the Risk Manager with the risk treatment subissue link. 8. System updates Risk Manager status board. 9. User adds the verification/monitoring/measurement subissue to the ISMS project. 10. System saves subissue 11. User complements the Risk Manager with verification/monitoring/measurement subissue link. 12. System updates the Risk Manager status board.
14.	Alternative scenario	5a. User adds the issue to relevant project to treat the risk. 5b. User links issue to the ISMS relevant issue (control)
15.	Related use cases	Based on Use case T-UC-5

Table 13. Use case I-UC-3

No.	Section	Content
1.	Identifier	I-UC-3
2.	Name	Generate SoA status Board
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	High
6.	Criticality	Assess status of SoA
7.	Source	BP-2 Compile SoA first version
8.	Short Description	General view of issues related to the ISMS SoA project and related projects
9.	Goal(s)	G0-11, G0-10, G0-4, G0-09
10.	Actor(s)	ISMS Authority
11.	Precondition	ISMS project is created
12.	Postcondition	Ability to click on issue to see issue info.
13.	Main scenario	1. User open the ISMS project. 2. System displays the ISMS project info. 3. User selects to see the project status board. 4. System displays ISMS project subissues. 5. User selects to see the other project linked issues on the board. 6. System adds the selected project issue to the display. 7. User filters the issues to be shown on the board. 8. User saves the report filters for further use. 9. System saves the report filters and displays the filtered issues.
14.	Alternative scenario	-
15.	Related use cases	-

Table 14. Use case P-UC-1

No.	**Section**	**Content**
1.	Identifier	P-UC-1
2.	Name	Generate project management SoA
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	High
6.	Criticality	To gather the ISMS requirements.
7.	Source	BP-5 Project management
8.	Short Description	User creates from SoA controls issues into his the project.
9.	Goal(s)	G0-4, G0-09, G0-7
10.	Actor(s)	Project manager
11.	Precondition	Organization SoA is created (Use case I-UC-1), project is created
12.	Postcondition	Project has the issues from the SoA.
13.	Main scenario	1. User imports SoA controls list to his project. 2. System creates issues.
14.	Alternative scenario	1a. User links his project to ISMS project 2a. System offers to use the SoA as a template to generate issues. Proceed to step 2. 3a- Use case P-UC-2
15.	Related use cases	includes Use case P-UC-2

Table 15. Use case P-UC-2

No.	Section	Content
1.	Identifier	P-UC-2
2.	Name	Select applicable controls
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	Medium
6.	Criticality	For futher work effectiveness
7.	Source	BP-5 Project management
8.	Short Description	User selects relevant controls from the approved SoA to his project(s). User marks the non-applicable controls to his projects with the justification and generates the issues only from the applicable controls.
9.	Goal(s)	G0-10, G0-4, G0-09, G0-7, To get Project(process based SoA), to integrate information security controls into organization processes
10.	Actor(s)	Project (process) Manager
11.	Precondition	Project SoA is generated (Use case P-UC-1)
12.	Postcondition	Project based SoA list (with applicable and non-applicable control) is saved and issues are generated.
13.	Main scenario	1. User marks controls to be applicable or nonapplicable. 2. User writes the justification into description of non-applicable controls. 3. User applies the result. 4. System updates the project based SoA status. 5. System creates the issues for applicable controls. 6. System relates applicable issues to the ISMS project based on Standard ID custom field value.
14.	Alternative scenario	6a. System relates applicable issues subissues to be the subissues of the corresponding issues in the ISMS project 5b. Use case P-UC-3 Proceed on step 5.
15.	Related use cases	inclusion of Use case P-UC-1, inclusion of Use case P-UC-3

Table 16. Use case P-UC-3

No.	Section	Content
1.	Identifier	P-UC-3
2.	Name	Save project-SoA controls template
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	Medium
6.	Criticality	To define the project based information security management requirements
7.	Source	BP-5 Project management
8.	Short Description	User saves marked project(process) based controls from the ISMS project SoA to use them for the current project and as the template for further created projects.
9.	Goal(s)	G0-9, G0-4
10.	Actor(s)	Project Manager
11.	Precondition	Applicable project/process controls are selected (realised Use case P-UC-2)
12.	Postcondition	Project based SoA template is saved for further use.
13.	Main scenario	1. System provides to save the result of issues list to be a template. 2. User chooses the issues list to be a "template". 3. System asks the template name and description. 4. User names the template and writes the description of template. 5. System saves the template in the project templates list.
14.	Alternative scenario	2a. User chooses not to save the template. Proceed to Use case P-UC-2. 2b. User exports the project SoA issues for further templates. 3b. System download the exported SoA issues file. 4b. User names the file and uploads it in project/process description. 5b. System updates the project/process description.
15.	Related use cases	inclusion of Use case P-UC-2

Table 17. Use case P-UC-4

No.	Section	Content
1.	Identifier	P-UC-4
2.	Name	Update project description
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	Medium
6.	Criticality	Gives the verification of ISMS integration to projects(processes)
7.	Source	BP-5 Project management, BP-7 Compile SoA
8.	Short Description	User updates project general description with ISMS related data, which is accessible to the project members
9.	Goal(s)	G0-11, G0-10, G0-4, G0-7 Trace project information security requirements
10.	Actor(s)	Project Manager
11.	Precondition	Project is created
12.	Postcondition	Project description info is updated.
13.	Main scenario	1. User opens project description editor. 2. User chooses template to the project description. 3. User describes project info (in natural language): 3.1. Project information assets (input, output) 3.2 Requirements to the assets (C,I,A) 3.3 Related contacts (include NDA) requirements 3.3 Relation to the SoA controls list 4. System validates, that needed fields are fulfilled 5. System updates project description
14.	Alternative scenario	3a. User links relevant documents into project description fields (includes Use case S-UC-4 . Proceed to 4. Step 4b. System validation failed 5b. System gives a notification to user about violation of filling fields in template 6b. User fulfilles the missing fields. 6c. User refuses to fulfill fields. Proceed to 5. step 2d (skip step) Proceed to 3. step 4d (skip step) Proceed to 5. step
15.	Related use cases	includes Use case S-UC-4

Table 18. Use case S-UC-1

No.	Section	Content
1.	Identifier	S-UC-1
2.	Name	S-UC-1 Generate printable SoA
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	Medium
6.	Criticality	Auditor or a third party has right to get SoA to add to audit report. Organization needs to be able to organize on the request printable version of the last SoA.
7.	Source	BP-7 Compile SoA
8.	Short Description	User requires system to generate SoA last version
9.	Goal(s)	G0-11, G0-7 Export SoA document
10.	Actor(s)	ISMS Authority
11.	Precondition	SoA issues are created.
12.	Postcondition	SoA is exported/downloaded.
13.	Main scenario	1. User opens ISMS project description. 2. User finds SoA last (approved) version. 3. User selects to export the SoA. 4. System downloads the SoA.
14.	Alternative scenario	3a. User selects to print the SoA. 4a. System sends SoA to printer dialog. 3b. User selects features to print (Use case S-UC-2) Proceed to the step 3. 3c. User select to link SoA to project description Use case S-UC-4 Proceed to the step 3.
15.	Related use cases	includes Use case S-UC-2, includes Use case S-UC-4

Table 19. Use case S-UC-2

No.	Section	Content
1.	Identifier	S-UC-2
2.	Name	S-UC-2 Filter objects to show in SoA
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	Medium
6.	Criticality	Depends on the user organization needs
7.	Source	BP-7 Compile SoA
8.	Short Description	During the SoA generation user selects the features to show in the SoA.
9.	Goal(s)	G0-11, G0-7 To customize SoA by the usage (external/internal).
10.	Actor(s)	ISMS Authority, Project Manager
11.	Precondition	SoA issues are created
12.	Postcondition	SoA exportable/printable version features are selected
13.	Main scenario	1. Use case S-UC-1 User opens the SoA for export 2. System provides features to include in the SoA. 3. User selects optional features for SoA. 3.1. Mandatory features: Control summary (with Standard notation), status (A/NA), approve date and version 4. System creates SoA with selected features
14.	Alternative scenario	3a. User does not make a selection. 4a. The system creates SoA with mandatory features.
15.	Related use cases	inclusion to Use case S-UC-1

Table 20. Use case S-UC-3

No.	Section	Content
1.	Identifier	S-UC-3
2.	Name	Update version number of SoA
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	High
6.	Criticality	To keep traceability of versions
7.	Source	BP-7 Compile SoA
8.	Short Description	System updates the SoA version number after management have approved SoA.
9.	Goal(s)	G0-11, G0-7 Fix last SoA version
10.	Actor(s)	ISMS Authority
11.	Precondition	Use case S-UC-1
12.	Postcondition	SoA last version is fixed
13.	Main scenario	1. User edits the SoA meta-data 2. System provides to user to change date of last confirmation. 3. System provides new version number to SoA. 4. User approves dates and version number. 5. System updates project description (Use case S-UC-4).
14.	Alternative scenario	1a. User adds version number, date of last approval manually 2a. System updates project description
15.	Related use cases	based on Use case S-UC-1

Table 21. Use case S-UC-4

No.	Section	Content
1.	Identifier	S-UC-4
2.	Name	Link SoA to ISMS project description
3.	Author	Mari Seeba
4.	Change history	26.03.2019
5.	Priority	Medium
6.	Criticality	Users know which controls are applicable
7.	Source	BP-7 Compile SoA
8.	Short Description	User links approved version of the SoA to the ISMS project description.
9.	Goal(s)	G0-11
10.	Actor(s)	ISMS Authority
11.	Precondition	Use case S-UC-1, Use case S-UC-3, Use case P-UC-4
12.	Postcondition	Dated and with the version number SoA is linked to the ISMS project description.
13.	Main scenario	1. User selects SoA last version to include into project info. 2. System updates project description. 3. User opens linked document to verify result. (Optional)
14.	Alternative scenario	1a. User adds link to the project description of the SoA. 2a. System updates the project description. 3a. User generates the SoA by clicking on the link. 4.a System displays SoA.
15.	Related use cases	includes Use case S-UC-1, inclusion to Use case P-UC-4

C.7 ISMS tool components

Figure 32 illustrates the ISMS tool system objects classes and the relationships of the classes. Object classes descriptions are listed in natural language:

Issue The issue is a requirement to follow by an assignee, who can change issue status, assignee, description and add links. Issue is and object in the Use case T-UC-1, Use case T-UC-2, Use case T-UC-3 , Use case T-UC-4 , Use case T-UC-5 , Use case I-UC-1, Use case P-UC-2

Project Project generalizes types of projects (all of them are not included on the diagram). Each project has description. Project class has a collection of Issues. Project is an object in the Use case T-UC-3 , Use case I-UC-1, Use case I-UC-3, Use case E-UC-1, Use case S-UC-1, Use case S-UC-2, Use case S-UC-3, Use case S-UC-4 , Use case P-UC-1, Use case P-UC-2, Use case P-UC-3,Use case P-UC-4.

ISMSProject ISMS Project is a project where an organization manages ISO27001 requirements as issues to which in turn are added documents links. ISMS Project improvement needs are subissues of relevant issues. ISMS Project description includes SoA - a fixed version of SoA issue statuses (applicable/nonapplicable) with justifications for nonapplicable issues. This SoA can be used as SoA template to import into projects project-based SoA issues. ISMS Project is and object in the Use case I-UC-1, Use case S-UC-4 , Use case P-UC-4, Use case P-UC-1, Use case P-UC-2, Use case S-UC-1

Business Process Project The project is meant to be a project or process included in the ISMS scope. Project description includes:

1. Information assets (input, output)
2. Requirements to the assets (C, I, A)
3. Related interested parties
4. Regulative, legal and contractual requirements
5. Related non-disclosure agreement (NDA) requirements
6. Relation to controls list template (depends on the project)

These artifacts can be links to the separate documents. This list is incomplete and can differ by internal procedures. SoA issues in the project are importable from SoA template. Non-applicable SoA issues for that project can be marked as non-applicable during the import process. However, these issues require justification in the description field of why they are non-applicable. Business process Project is an object of the Use case I-UC-1, Use case S-UC-4 , Use case P-UC-4, Use case P-UC-1, Use case P-UC-2,Use case P-UC-3

ISMSRiskManager Risk Manager Jira adds-on is developed by SoftComply. Here RiskManager is an independent object, which have functionality for risk assessment, risk treatment, and verification traceability and risk management model. ISMS Risk manager handles risks in information security management system. Risk Manager is an object in the Use case I-UC-2.

SecurityEventIssue Security Event Issue is a special issue type in incident management project. Security event issues are basing on the issue template. The issue should have Standard notation ID to tie it to Risk Manager. Then it also should be related to SoA project issue trough Standard ID. Issue workflow: ToDo, assess, in progress, evaluate, Done. Security event issue is an object in the Use case E-UC-1.

SoA SoA is a formal version of SoA status report (board). SoA gives an overview of organization decision of applicable and non-applicable ISO27001 and ISO27001 Annex A controls. SoA printable/downloadable version is a base for the template which is used in other projects as SoA issues template. SoA is an object in the Use case P-UC-1, Use case P-UC-2, Use case S-UC-4 , Use case S-UC-1, Use case S-UC-2, Use case S-UC-3, Use case S-UC-4

SoAIssue SoA issue is one-to-one ISO27001 main part or Annex A requirement in ISMS project. SoA issue status is applicable or non-applicable and in case of applicable links required process description and policies. At the very beginning, the status could be as ToDo. If Standard changes, then the status of the issue could be Closed. SoA issue is and object in the Use case T-UC-1, Use case T-UC-2, Use case T-UC-3 , Use case T-UC-4 , Use case T-UC-5 , Use case I-UC-1, Use case P-UC-2

SoaSubIssue SoA subissue is an issue in ISMS project. Subissue is directly related to issue by Standard ID (ISO27001 notation). SoA subissues contain evidence links and decisions to trace ISMS activities. SoA subissue is an object in the Use case T-UC-1, Use case T-UC-3 , Use case T-UC-5 .

SoAStatusReport SoA status report is an overview board of ISMS project subissue statuses. SoA status board report is an object in the Use case I-UC-3,

SoATemplate SoA template is a collection of issues based on ISO27001. Issues statuses are set to be applicable (with relevant links to documents) or non-applicable (with justification). SoA template is generated from the ISMS project issues and contains the SoA version number. SoA template is and object in the Use case I-UC-1, Use case P-UC-3, Use case S-UC-1, Use case S-UC-4

ProjectSoAIssue Project SoA issue is type of project issue which has statuses applicable or non-applicable, its subissues describe using points and evidence of SoA issue implementation in the project. Project SoA subissue is and object in the Use case T-UC-1, Use case T-UC-2, Use case T-UC-3 , Use case T-UC-4 , Use case T-UC-5 , Use case I-UC-1

ProjectSoASubissue Project SoA subissue collects evidence of how this project manages parent issues requirements and rules. Project SoA subissue is and object in the Use case T-UC-1, Use case T-UC-2, Use case T-UC-3 , Use case T-UC-4 , Use case T-UC-5 , Use case I-UC-1

ProjectSoATemplate Project SoA Template is a collection of SoA issues relevant to the specific type of projects. Project SoA template bases on SoA, where non-applicable issues are marked to be non-applicable and other issues are to manage and to produce evidence of the performace. Project SoA template is and object in the Use case I-UC-1, Use case P-UC-3, Use case S-UC-1, Use case S-UC-4

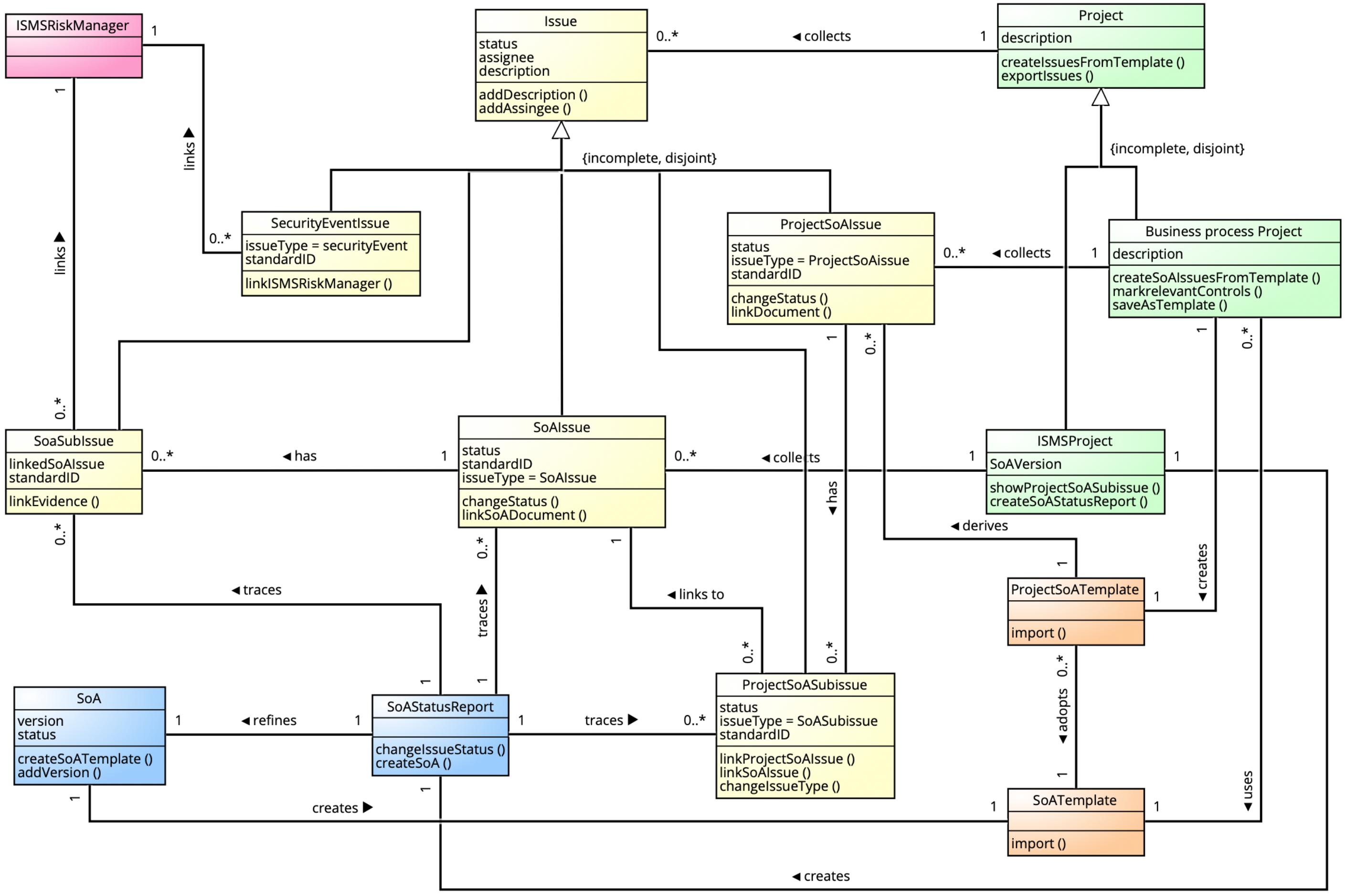


Figure 32. ISMS tool objects class diagram

Non-exclusive licence to reproduce thesis and make thesis public

I, **Mari Seeba**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   A Specification of Layer-Based Information Security Management System for the Issue Tracking System

   supervised by Prof Raimundas Matulevičius and Prof Ahto Buldas.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Mari Seeba
Tartu, 16.05.2019