TARTU ÜLIKOOL
Arvutiteaduse instituut
Infotehnoloogia mitteinformaatikutele õppekava

Kadri Koit

Eesti infoturbe standardi (E-ITS) nõuete kirjeldamine riigihangetes

Magistritöö (15 EAP)

Juhendaja Kristjan Krips, PhD

Tartu 2024

Eesti infoturbe standardi (E-ITS) nõuete kirjeldamine riigihangetes

Lühikokkuvõte:

Eesti, üks maailma kõige digisõltuvamatest riikidest, seisab silmitsi oluliselt suuremate küberohtude mõjudega võrreldes paljude teiste riikidega. Selles kontekstis on Eesti riik vastanud kasvavatele turvanõuetele, kehtestades uue Eesti infoturbestandardi (E-ITS). E-ITS on mõeldud infoturbe tõhusamaks juhtimiseks nii suurtes kui väikestes organisatsioonides. Standardi rakendamise kohustus on kõigil Küberturvalisuse seaduse kohaldamisalasse kuuluvatel organisatsioonidel alates 2023. aasta jaanuarist. Paljud nendest organisatsioonidest ei oma enam oma IT-infrastruktuuri ning hangivad IT-teenused välistelt teenuseandjatelt. Standardi uudsus on tekitanud olukorra, kus hangetes viidatakse veel varasemalt kehtinud ISKE süsteemile, näidates üleminekuperioodi keerukusi ja väljakutseid. Teisalt on tekkinud ka probleem hanke tehnilise kirjelduse üldsõnalisusega, millega on tekkinud olukord, kus ei ole üheselt selge, kes on turvameetmete rakendamise eest vastutav osapool. Magistritöö eesmärk oli pakkuda üks võimalik lähenemisviis, kuidas aidata hankijatel kirjeldada IKT teenuste hankes infoturbe meetmete tehnilised tingimused. Magistritöö käigus koostatud kontrollnimekirjade komplekt aitab hankijatel määratleda nende organisatsiooni turvapoliitikatele vastavad infoturbe meetmed, mille täitmist teenuseandjatelt hangitava teenuse raames küsida, pakkudes sellega metoodilist tuge riigihangete tehniliste kirjelduste koostamiseks.

Võtmesõnad:

Eesti infoturbe standard, riigihange.

CERCS: P175 Informaatika, süsteemiteooria

Describing the Requirements of the Estonian Information Security Standard (E-ITS) in Public Procurements

Abstract:

Estonia, one of the world's most digitally dependent countries, confronts significantly greater repercussions from cyber threats compared to many other nations. In response to this pressing challenge, the Estonian government has introduced the new Estonian Information Security Standard (E-ITS), aimed at bolstering information security management across enterprises of varying scales. The obligation to implement the standard applies to all organizations within the scope of the Cyber Security Act, effective from January 2023. A considerable proportion of these entities no longer maintain their own IT infrastructure and procure IT services from external service providers. However, the introduction of the standard has created a conundrum where procurement processes still make reference to previously applicable ISKE system, indicating the complexities and challenges of the transition period. On the other hand, there exists an issue pertaining to the vagueness in the technical specifications of procurements, resulting in ambiguity regarding the party responsible for implementing security measures. The aim of the master's thesis was to provide one possible approach to help procurers define the technical requirements for information security measures in ICT service procurements. The compendium of checklists developed during the master's thesis helps procurers define information security measures aligned with their organization's security policies, which can be requested from service providers within the scope of the services procured, thereby providing methodological support for drafting technical specifications in public procurements.

Keywords:
Estonian Information Security Standard, public procurement.
CERCS: P175 Informatics, systems theory

Sisukord

Terminid ja lühendid

ASVS – Application Security Verification Standard (eesti keeles rakenduste turbe verifitseerimise standard)
ANSI – American National Standards Institute (eesti keeles Ameerika Standardiinstituut)
ASLR – address space layout randomization (eesti keeles aadressiruumi juhustus)
BSI IT-Grundschutz – Saksa Liidumaa riikliku infoturbeameti IT baastaseme kaitse
CIS – Center for Internet Security
DEP/NX –Data Execution Prevention or No-Execute
E-ITS – Eesti Infoturbestandard
EHIS – Eesti Hariduse Infosüsteem
ETIS – Eesti Teadusinfosüsteem
ETO – elutähtsa teenuse osutaja
GDPR – General Data Protection Regulation (eesti keeles isikuandmete kaitse üldmäärus)
GID – group ID (eesti keeles rühmanimi)
IKT – info- ja kommunikatsioonitehnoloogia
IaaS – infrastructure as a service (eesti keeles taristu teenusena)
ICMP – Internet Control Message Protocol (eesti keeles interneti juhtsõnumiprotokoll)
ICMPv6 – Internet Control Message Protocol version 6 (eesti keeles interneti juhtsõnumiprotokoll 6 versioon)
IEC – International Electrotechnical Commission (eesti keeles Rahvusvahelise Elektrotehnika Komisjon)
ISKE – infosüsteemide kolmeastmeline etalonturbe süsteem
ISO – International Organization for Standardization (eesti keeles Rahvusvaheline Standardiorganisatsioon)
ISMS – information security management system (eesti keeles infoturbe halduse süsteem)
ITIL – Information Technology Infrastructure Library (eesti keeles infotehnoloogia taristu teek)
KEMIT – Keskkonnaministeeriumi Infotehnoloogiakeskus
KüTS – Küberturvalisuse seadus
OWASP – The Open Worldwide Application Security Project (eesti keeles avatud veebirakenduste turbe projekt)
P-A-P – paketifilter-rakenduslüüs-paketifilter
PEARO – Pole asjakohane; Ei ole rakendatud; Aktsepteeritud risk; Rakendatud; Osaliselt
RIA – Riigi Infosüsteemi Amet
RMK – Riigi Metsamajandamise Keskus
SIEM – Security Information and Event Management (eesti keeles turbeteabe ja -sündmuste haldus)
SLA – Service Level Agreement (eesti keeles teenusetaseme lepe)
SoCaas – Security Operation Center as a Service (eesti keeles turbehalduskeskus teenusena)
SSH – Secure Shell (eesti keeles turvaline kest)
SYN – synchronization (eesti keeles sünkroniseerimine)
TCP – Transmission Control Protocol (eesti keeles edastusohje protokoll)
TSL – Transport Layer Security (eesti keeles transpordikihi turve)
UDP – User Datagram Protocol (eesti keeles kasutajadatagrammi protokoll)
UID – unique identifier (eesti keeles ühene identifikaator)
VLAN – virtual local area network (eesti keeles virtuaalne kohtvõrk)
VPN –virtual private network (eesti keeles virtuaalne privaatvõrk)

Sissejuhatus

Ettevõtted ja organisatsioonid sõltuvad tõhusalt tegutsemiseks ning teadlike otsuste tegemiseks olulisel määral andmetest. Digitehnoloogiate rakendamine võib anda konkurentsieelise, kuid sellega kaasneb sõltuvus IT süsteemidest, mistõttu tuleb tagada IT süsteemide turve. Küberkuritegevuse kasv on asetanud nii era- kui avaliku sektori organisatsioonid surve alla ja toonud esile praeguste tegevuste või tegemata jätmiste puudujäägid ning kitsaskohad küberturbe valdkonnas. Riigi Infosüsteemi Ameti (RIA) 2023. aastat kirjeldava küberturvalisuse aastaraamatu artikkel „Olukord küberruumis: ummistusrünnete aasta kordus" teeb ülevaate CERT-EE poolt tuvastatud mõjuga intsidentidest: kõikvõimalike õngitsusi teavitati 1722 korral, registreeriti 546 pettust, 312 teenusekatkestuse juhtu, 207 korral teavitati kasutajakonto ülevõtmistest, 165 korral andmete kompromiteerimisest ja registreeriti 139 teenusetõkkerünnakut [1].

Infoturbe meetmete kasutuselevõtmine võimaldab riske vähendada, kuid ei eemalda täielikult negatiivsete stsenaariumite juhtumise tõenäosust. Organisatsioonidel on keeruline olla teadlik uutest ohtudest ning olla valmis potentsiaalseks rünneteks. Infoturbe valdkonnas eksisteerib tuhandeid ohte ja miljoneid tuntud rünnakute vektoreid. Infoturbe integreerimine äriprotsessi võib osutuda keeruliseks, eriti kui asutus pole sellega varem kokku puutunud.

Alates 2023. aasta jaanuarist kehtib Eestis uus Eesti infoturbestandard (E-ITS). E-ITS loob aluse infoturbe paremaks juhtimiseks, panustades ühtlasi Eesti e-riigi turvalisse toimimisse. E-ITSi rakendusjuhendis on üheks eesmärgiks toodud arendada ning tõsta nii avaliku sektori kui ka erafirmade infoturbe taset [2]. E-ITSi rakendamine aitab edendada organisatsioonide infoturbealast kompetentsi ning muudab infoturbe tegevused jõukohasemaks ka väiksematele organisatsioonidele. Eelnevalt kasutusel olnud kolmeastmelise infosüsteemide turvameetmete süsteemi (ISKE) rakendamine oli mahukuse tõttu väiksemate organisatsioonide jaoks keeruline.

Küberturbe kujundamine ettevõtte äritegevuse strateegiliseks toetamiseks eeldab mitmete komponentide põhjalikku läbimõtlemist. Vastavalt Eesti Infoturbe standardi rakendusjuhendile hõlmab see varade kaardistamist, turbeprotsesside kavandamist, äriprotsesside kaardistamist, riskijuhtimist ning turvameetmete kinnitamist ja käigushoiu poliitikate väljatöötamist [2]. Ettevõtlus- ja infotehnoloogiaministri määruses „Eesti infoturbestandard" on seatud infoturbe peamiseks eesmärgiks tagada avalike ülesannete täitmiseks kasutatavate äriprotsesside ja infosüsteemide kõikehõlmav kaitse [3].

Viimaste aastate arengud digitaliseerimisel on suunanud paljud asutused kasutusele võtma teenuseandjate lahendusi oma serverite ja nende haldamiseks vajaliku oskusteabe omamise asemel. Erinevalt paljudest ettevõtetest on teenuseandjatel suurem võimekus palgata ning koolitada kvalifitseeritud tööjõudu, mis lihtsustab teenuse tarbija jaoks vajaliku funktsionaalsuse kasutuselevõttu. Sellega seoses on teenuseandja ja kliendi vaheline koostöö muutunud üliloluliseks ka küberturvalisuse vaates. Kõige kriitilisem on selle koostöö juures küsimus – kes kannab vastutust kui toimub küberturbe intsident.

Riigiasutused tellivad teenuseid hangete kaudu ning hangetes tuleb määratleda ka infoturbega seonduv. Koostöö valguses on vajalik, et hangete tehnilistes kirjeldustes esitatud nõuded teenuseandjatele oleksid piisavalt täpsed ja ajakohased. Tänased hangete tehnilistes kirjeldustes toodud nõuded teenuseandjatele tellitava IT-teenuse küberturvalisuse tagamiseks

varieeruvad üldsõnaliste kirjelduste ning viidetega varem kehtinud ISKE (infosüsteemide kolmeastmeline etalonturbe süsteem) vahel. Magistritöö eesmärk oli koostada kontrollnimekirjade komplekt, mis aitab hankijal kirjeldada hankes teenuseandjatelt nõutavaid tehnilisi turvameetmeid. Töö raames kirjeldati E-ITSi ja teiste E-ITSiga relevantsete standardite olemust, kirjeldati riigihanke protsessi ning analüüsiti riigihankeid. Autor on kontrollnimekirjade komplekti koostamisel aluseks võtnud E-ITSi rakendusjuhendi, arvestades sealjuures standardset hankeprotsessi ja organisatsiooni infoturbe küpsustaset. Kontrollnimekirjade komplekt pakub hankijale metoodilist alust teenuseandja vastutusalas olevate infoturbe meetmete sõnastamiseks. Kontrollnimekirjade komplekti praktilisel rakendamisel peab hankija arvestama konkreetse teenuse sisuga. Autorile teadaolevalt puuduvad varasemad juhised turvameetmete kirjeldamiseks riigihangete kontekstis, tehes selle teema uurimise aktuaalseks.

Magistritöö koosneb sissejuhatusest, seitsmest peatükist, kokkuvõttest, kasutatud kirjanduse loetelust ja lisadest. Esimeses peatükis esitatakse probleemipüstitus, tuuakse välja töö eesmärk, määratletakse töö käsitlusala, eeldatavad tulemid ja kirjeldatakse autori rolli. Teises peatükis antakse ülevaate magistritööga seotud infoturbe standardistest. Kolmandas peatükis antakse ülevaate E-ITSi ja riigihangetega seotud seadustest ja määrustest. Neljandas peatükis kaardistatakse riigihanke protsess. Viiendas peatükis tuuakse näiteid 2023. aastal väljastatud riigihangetest ning analüüsitakse kahte hanget. Kuuendas peatükis esitatakse kontrollnimekirjade komplekt. Seitsmendas peatükis antakse ülevaade huvitatud osapooltega teostatud intervjuude tulemustest. Lisades on toodud hangete põhjalik analüüs ja teostatud intervjuude küsimused ning nende pikemad kokkuvõtted.

1. Ülesandepüstitus

Autor esitleb käesolevas peatükis probleemi kontuurid, kirjeldab töö eesmärki ja selle saavutamiseks kavandatud tegevusi. Autor annab ülevaate töö vajalikkusest, tutvustab töö käsitlusala ning defineerib autori positsiooni uurimisprotsessis.

1.1 Probleemi kirjeldus

Organisatsioonide küberturbe taseme tõstmiseks on riik ühe meetodina välja töötanud uue infoturbe standardi Eesti Infoturbe Standard (lühidalt E-ITS), mis pakub suuniseid kaardistamaks organisatsioonide äriprotsesse ja varasid ning määratlemaks nende kõike hõlmava kaitsetarbe.

E-ITSi rakendamine on kohustuslik kogu Küberturvalisuse seaduse kohaldamisalale [4]. Mitmed neist organisatsioonidest, kellele seadus kohaldub, ei oma enam oma IT-infrastruktuuri ning eelistavad hankida IT-teenused välistelt teenuseandjatelt. E-ITSi määrus muutus kohustuslikuks 2023. aasta jaanuaris, kuid pärast seda tähtaega avaldatud riigihangetes on siiski viidatud eelnevalt kehtinud infosüsteemide kolmeastmelise etalonturbe süsteemile (ISKE), mille kehtivus lõppes 31. detsembril 2022. Hangetes ei pruugita alati täpsustada nõudeid teenuseandjalt tellitava teenuse infoturbe taseme määratlemiseks või on nõuded üldsõnalised ning võimatud teenuseandjal täita.

RIA 2022. aastat kirjeldavas küberturvalisuse aastaraamatus on esitatud RIA järelevalveametnike [5] vaatenurgast nõuete täitmise seis, millest joonistuvad välja kolm peamist probleemi: puudub süsteemne lähenemine infoturbele ja IT-riskihaldusele; võrgu struktuuri ebaotstarbekus ning selle kohta asjakohase dokumentatsiooni nappus; vananenud taakvara kasutamine, vähesed pingutused võrguseadmete turvanõrkuste tuvastamisel ja kõrvaldamisel, sealhulgas tootjapoolse toeta tarkvara kasutamine ning paikamata haavatavused süsteemides.

1.1.1 E-ITSi rakendamise raskused

Murekohtade hulgas on ka ISKE rakendajad: ehkki ISKEst lähtuvad andmekogude kontseptsioonid ja nendele rakendatavad turvaklassid tunduvad olevat ülekantavad ning sobilikud ka E-ITSi rakendamiseks, ei ole ISKE ja E-ITS oma rakendamise poolest täielikult samaväärsed. Näiteks äriprotsessi kaitsetarve võib oluliselt erineda kasutatava andmekogu turvaklassist. ISKE vastavustabel E-ITSile on informatiivse iseloomuga, nagu sõnab ka E-ITSi vastavustabelite veebilehel olev hoiatus [6]. Meetmete rakendatuse ülekandmine ISKEst E-ITSi ei ole soovitatav nende meetmete erinevuse tõttu, kuna vastavustabel kehtib ainult esimese, E-ITS 2020. aasta versiooni jaoks.

E-ITSi kontseptsioonimoodul, mis käsitleb välisteenuste tellimist, määratleb teenuseandja valimise kriteeriumid ja kokkulepete vajadusi [7]. Lisaks peab teenuseandja tagama, et tellijal oleks juurdepääs vajalikule teabele ja auditeerimisvõimalustele nõuete täitmise kontrollimiseks. Siiski jätab moodul määratlemata, kuidas teenuseandja peab oma süsteeme kaitsma, mis toob kaasa tellija ja teenuseandja vastutuse piiride ebamäärasuse.

RIA 2022. aastat kirjeldavas küberturvalisuse aastaraamatus märgitakse, et 2023. aasta alguses jõustunud uue infoturbe standardi rakendamine esitab väljakutse ligikaudu 3500 asutusele, kes täidavad avaliku sektori ülesandeid või osutavad kriitilisi teenuseid. Standardi rakendamine on üks meetod teenuste kaitseks [8]. Organisatsiooniliste äriprotsesside põhjalik mõtestamine,

riskipiirkondade kindlakstegemine, plaanide koostamine ning infoturbe taseme määratlemine on kriitilise tähtsusega, kuna IT-süsteemide intsident võib mõjutada kogu organisatsiooni toimimist ja käekäiku.

1.2 Magistritöö aktuaalsus ja vajalikkus

Käesolev magistritöö pakub uudset lähenemist, kuidas hankija teenuse tellijana defineerib konkreetsed meetmed, mille rakendamist teenuseandjalt ootab. Autori teadmiste kohaselt ei ole varem koostatud lõputöid, mis käsitleksid E-ITSi mooduleid antud vaatenurgast. Magistritöö raames loodud teadmust saab ära kasutada täiendades hankes osalevate osapoolte teadlikkust ning eeldusi teenuseandja pakutava teenuse osas. Magistritöö aitab senisest täpsemini määrata turvameetmete rakendamise eest vastutavad osapooled. Lõppeesmärgiks on soodustada E-ITSi efektiivset rakendamist.

Tuginedes seadusandlusele ja autori hinnangule teenuseandja võimekusele tagada hankija tellitavate IT-teenuste turvameetmete rakendamine, on autor koostanud hanke kontrollnimekirjade komplekti näidise, mis on esitatud seitsmendas peatükis. Soovituslike turbemeetmete kontrollnimekirjade komplekt võimaldab hankijal defineerida selgelt vajalikud turbemeetmed ning teenuseandjal pakkuda hankija nõuetele ja soovidele vastavat teenust. Ühtne arusaam turbemeetmetest ja vastutajatest lihtsustab hankeprotsessi ja tõstab infoturbe taset.

Eduka IKT-hankeprotsessi eelduseks on hankijapoolne põhjalik ülevaade organisatsiooni dokumentatsioonist ja äriprotsessidest. See tagab selgema arusaama vastutusaladest, mis omakorda parendab avaliku sektori hangete kvaliteeti ning tellitavate teenuste turvalisuse taset. Kohustus turvameetmete rakendamiseks lasub organisatsioonil endal, see tähendab, et asutus vastutab ka teenuseandja pakutavate teenuste infoturbe tagamise eest, on toodud välja RIA küberturbe 2022. aastat kirjeldavas aastaraamatus [9].

1.3 Eesmärk ja tegevused eesmärgi saavutamiseks

Käesoleva magistritöö eesmärk on pakkuda ülevaade E-ITSi kasutamisest IKT-teenuste riigihangetes ning tulemina koostada parimatest praktikatest koosnev kontrollnimekirjade komplekt hanke tehnilise kirjelduse koostamiseks. Komplekt sisaldab tegevusi selgitamaks välja, millised on E-ITSis kirjeldatud infoturbe meetmed, mille täitmist võib hankija teenuseandja käest küsida hanke koostamisel.

Autor kasutas töö eesmärgi – kontrollnimekirjade komplekti koostamiseks 2023. aastal avaldatud kahe riigihanke analüüsi. Analüüsi käigus kirjeldati, kui suurel määral on vaatluse all olevates hangetes nõutud vastavust E-ITSi rakendamisele teenuse osutamisel. Ühtlasi kaardistati, millised nõutud turvameetmed on võimalik teenuseandjal täita, mis ulatuses lasub kohustus hankijal ning millised on mõlema osapoole ühised vastutusvaldkonnad. Kontrollnimekirjade komplekt põhineb E-ITSi rakendusjuhendil, rahvusvahelise standardi ISO/IEC 27002 kontrollidel ja riigihanke protsessil. Töö raames koostas autor näidised Kubernetese ja veebiserveri teenuse meetmete vastutaja defineerimiseks. Kontrollnimekirjade komplekti eesmärk on toetada hanke tehnilise kirjelduse koostamist küberturbe meetmete kontekstis.

Näidishangete analüüsiga kaardistati olemasolevates hangetes soovitud infoturbe meetmete tehniliste kirjelduste ja teenuseandjate rakendamise võimalike meetmete täitmise vahelisi kitsaskohti ning valideeriti koostatud kontrollnimekirjade komplekti kasutatavust

teenuseandjatega Telia Eesti AS, Primend OÜ ja Tietoevry Estonia AS ning hankijatega Tallinna Strateegiakeskus, Riigimetsamajandamise Keskus ja Eesti Raudtee.

Magistritöö kirjeldab kolme etappi:
▪ esimese etapi moodustas olemasoleva olukorra kirjeldamine (*AS-IS*), mille raames loodi erinevate standardite ja seaduste kokkuvõte ning kirjeldati hankeprotsessi. Lisaks anti ülevaade hangetes kasutatavatest E-ITSi/ISKE meetmetest;
▪ teise etapi moodustas hangete analüüs turvameetme rakendamise eest vastutava osapoole määratlemiseks, riigihangetes E-ITSi rakendamise kontrollnimekirjade komplekti väljatöötamine ja modelleerimine (*TO-BE*);
▪ kolmanda etapi moodustas huvitatud osapoolte intervjueerimine parendusvõimaluste tuvastamiseks ja kontrollnimekirjade valideerimiseks.

1.4 Töö eeldatavad tulemid ja autori roll

Eeldatava tulemina koostas töö autor hankijale mõeldud juhise, mis aitab koostada hanke tehnilisse kirjeldusse minevaid küberturbe nõudeid ning kasvatab hankija teadlikkust. Kontrollnimekirjade näidiste koostamiseks töö autor:
▪ kaardistas hankija jaoks vajalikud tegevused uue IKT-teenuse hankimisel E-ITSi rakendamise kontekstis;
▪ tuvastas turvameetmete eest vastutavad osapooled kahe erineva teenuse näitel.

Töö kajastab autori isiklikke seisukohti, mis ei pruugi kattuda standardi omaniku, Riigi Infosüsteemi Ameti (RIA), seisukohtadega. Töö autor omab töö kirjutamise ajal mitmeaastast töökogemust IKT-teenuste müügijuhina. Antud ametikoha töökogemus on andnud autorile ülevaate erinevate IKT-teenuste sisust ning nende rakendamisest teenuseandja perspektiivist. See kogemus on olnud märkimisväärne allikas vastutusalade määratlemisel ja pakkunud väärtuslikku sisendit magistritöö probleemistiku lahendamisel. Eelpoolnimetatu on töö autori hinnangul piisav, et seda kasutada magistritöös esitatud seisukohtade põhjendamisel ja analüüsitulemuste sünteesimisel.

2. Standardid

Järgnev peatükk annab ülevaate lõputöö jaoks relevantsetest standarditest ning selgitab kuidas need on seotud riigihangetega. Riigihangete raames kasutatakse IKT-teenuseid tellides enim kolme standardit – E-ITSi selle rakendamise kohustuse poolest KüTSi mõjualas, ISKE-t ajaloolise tähtsuse tõttu Eesti infoturbe kontekstis ja ISO/IEC 27001 rahvusvahelise tuntuse ja laialdase rakendatavuse poolest. Kuigi Eestis läbiviidavatel riigihangetel ei viidata BSI IT-Grundschutz'ile, kuna selle baasil on loodud nii ISKE kui E-ITS.

2.1 Eesti Infoturbe Standard ehk E-ITS

RIA töötas välja Eesti Infoturbe Standardi (E-ITS) asendama ISKE-t. Standardi esimene versioon ilus aastal 2021. E-ITS on suunatud ennekõike avaliku sektori, kuid ka eraettevõtete infoturbe taseme tõstmiseks. E-ITSi eesmärk on tagada avalike ülesannete täitmiseks kasutatavate äriprotsesside ja infosüsteemide kõikehõlmav kaitse ning infoturbe ühtlane tase nende eelnimetatu kõigis osades [10]. E-ITSi haldajana ja omanikuna on määratletud RIA, kes vastutab standardi iga-aastase ülevaatuse ja uuendamise eest [10]. E-ITS tugineb Saksa Liitvabariigi BSI (*Das Bundesamt für Sicherheit in der Informationstechnik*) loodud IT-Grundschutz etalonturbele. E-ITSi tutvustatakse kui vahendit, mille eesmärk on pakkuda organisatsioonidele eestikeelne ja kohalikule õigusruumile vastav töövahend infoturbe käsitlemiseks, saavutamaks ettevõtte vajadustega sobiv infoturbe tase [11].

E-ITSi on tutvustatud ka RIA Küberturvalisuse 2022. aastat kirjeldavas aastaraamatus kui uuendatud standardit, mis on suunatud kasutamiseks, erinevalt 20 aastat kehtinud infoturbesüsteemist ISKE, laiemale sihtgrupile [9]. E-ITS kirjeldab meetmeid, mille järgimisel paraneb organisatsiooni toimepidevus, pakkudes süsteemset ülevaadet organisatsiooni (äri)protsessidest ja riskidest, suurendades samal ajal küberrünnakute ennetamise kui ka tagajärgedega toimetuleku võimekust.

E-ITS kujutab endast kaasaegset infoturbe raamistikku, mis on üles ehitatud eesmärgiga käsitleda infoturvet läbi äriprotsesside seades info- ja küberturbe rakendamisel fookusesse organisatsiooni terviklikult. Standardi lühitutvustuses on öeldud: „Organisatsioon peab olema teadlik oma eesmärkidest, põhikirjalistest ülesannetest ning suutma kirjeldada oma toimimise valdkondi, pakutavaid teenuseid äriprotsesside kaudu. Samuti peab organisatsioon olema teadlik riskidest, mis võivad tegevust takistada. E-ITS võimaldab organisatsioonil rakendada infoturbe parimaid praktikaid kõigile tegevusvaldkondadele ning seeläbi kokku hoida infoturbe rakendamisele kuluvaid vahendeid." [11]

21. detsembril 2022 Riigi Teatajas [12] avaldatud Eesti infoturbe standardi määrus kehtestab küberturvalisuse seaduse paragrahv 7 lõike 5 ning Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded" [13] paragrahv 3 lõike 1 alusel teenuse osutajale kohustuse võrgu- ja infosüsteemi turvalisuse tagamiseks järgida Eesti infoturbestandardit ja rakendada sellega seotud turvameetmeid. Nende määruste alusel tuleb teenuse osutajatel järgida E-ITSi nõudeid infoturbe halduse käivitamisel, rakendamisel, käigushoidmisel ja täiustamisel. Küberturvalisuse seadus (KüTS) vabastab kohustusest digitaalse teenuse osutajad, kellel on majandusaasta jooksul keskmiselt alla 50 töötaja ning kelle aasta bilansimaht või aastakäive ei ületa 10 miljonit eurot [4]. KüTSi paragrahvi 3 lõige 2 täpsustab, et teenuseosutaja, kes on rakendanud rahvusvahelist standardit ISO/IEC 27001 ning esitanud RIAle kehtiva vastavussertifikaadi, loetakse samuti nõuetele vastavaks [4].

Organisatsioonidele, kellele Küberturvalisuse seadus otseselt ei laiene, kuid kes peavad tagama küberturvalisuse muudest nõuetest tulenevalt, näiteks GDPR, soovitatakse selleks kasutada E-ITSi [14]. Ärinõustamisfirma KPMG täpsustab, et ka küberturvalisuse seadusele alluvatel erasektori asutustel on kohustus rakendada riskihaldust ja infoturbe meetmed, mis on kooskõlas E-ITSi või ISO/IEC 27001 standardi nõuetega [15].

E-ITS on loodud etalonturbe põhimõttele toetudes, tuginedes Saksa Liitvabariigi etalonturbe süsteemile BSI IT-Grundschutz ja ISO/IEC 27001:2014 „Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded" (27001) standardile [16]. Etalonturbe kontseptsiooni on kirjeldatud Mari Seeba poolt „Eesti infoturbestandard" Lisas 1 [3:15]: „Etalonturbe kontseptsioon lähtub põhimõttest, et infoturvaohud ja kaitstavad varad on erinevate organisatsioonide puhul tüüpsed. E-ITSi etalonturbe kataloog esitab moodulitesse koondatud eelanalüüsitud meetmekomplektid, mis katavad tüüpsete sihtobjektide riskihalduse ja infoturvavajadused." Standardi eesmärk on aidata organisatsioonil saavutada tema vajadustele sobiv infoturbe tase [17]. Etalonturbe standardit on tutvustatud kui turvameetmestikku, mille rakendamine on vajalik andmete turvalisuse saavutamiseks ja säilitamiseks, see on loodud seadmaks kaitstavad objektid ja protsessid vastavusse tüüpmoodulitega, mis kirjeldavad enamlevinud ohte ja nendega seotud turvameetmeid, mis on valitud riskianalüüsi põhjal [11]. Samas rõhutatakse ka juhtkonna rolli tähtsust protsessis, olles kaitsvate turbeprotsesside ja sihtobjektid määraja ning see ühtlasi seab ootused juhtkonnale infoturbe teadlikkuse, otsuste ja vastutuse osas [11].

E–ITSi etalonturbe kataloog on jaotatud kümneks valdkonnapõhiseid turvameetmeid sisaldavaks mooduligrupiks [11]:

- ISMS – turbehaldus, mis annab juhtnöörid katuse loomiseks ja korraldamiseks asutuses, sh juhtkonna kaasamiseks ja ressursside eraldamiseks turbele;
- ORP – organisatsioon ja personal, mis keskendub korralduslikule poolele ja inimeste ja õiguste haldusele ning koolitustele;
- CON – kontseptsioonid ja metoodikad, mis sisaldab alusprintsiipe, mille peale saab muid tegevusi ja kordasid luua ja millest lähtuda, nt varundamiste, arhiveerimiste, arendustööde vms korraldamisel;
- OPS – käidutööd, mis kirjeldab tegevusi, mida on vaja teha tarkvara ja riistvara ning võrgu halduseks ja mis on üldistatav üle mitmete tehniliste lahenduste;
- DER – avastamine ja reageerimine, mis juhendab asutusi turvaintsidentide halduse, auditite ja avariidega toime tulema;
- APP – rakendused, mis käsitleb tarkvara, rühmatöö vahendid ja tellimustarkvara haldamise teemasid;
- SYS – IT-süsteemid, mis käsitleb riistvaralisi lahendusi ja nende haldamise teemasid;
- IND – tööstuse IT, mis käsitleb tööpinkide juhtarvuteid, sensoreid, roboteid, labori- ja diagnostikaseadmeid, laosüsteeme, nende haldamist ning ohutust;
- NET – võrgud ja side, käsitleb võrgu, võrgukomponentide ja telefoniside haldamist;
- INF – taristu, mis käsitleb hoonete, ruumide, kaabelduste, mobiilsete töökohtade, sõidukite IT lahenduste, nn tarkade majade haldamist.

Standardi tutvustuses rõhutatakse, et infoturve ei kujuta endast ühekordset tegevust, vaid on pidev protsess, mis vajab regulaarset uuendamist kohanemaks ajas muutuvate ohtudega. Samuti soovitakse tutvustuses tagada organisatsiooni jätkusuutlikkus ja jälgitavus infoturbe halduse süsteemi (inglise keeles *Information Security Management System*, ehk ISMS) rakendamise kaudu [11]. ISMSi defineeritakse ISMS nõuete veebilehel kui organisatsiooni juhtimise osa, mis tegeleb infoturbe loomise, juurutamise, rakendamise, seire ja täiustamisega,

hõlmates organisatsiooni struktuuri, protsesse, protseduure, poliitikaid, kohustusi, ressursse ja varasid [10].

Eesti infoturbestandardi määruses „Nõuded infoturbe halduse süsteemile" on öeldud, et E-ITSi rakendamine standardturbe ulatuses võimaldab saavutada vastavuse rahvusvahelise standardiga ISO/IEC 27001 [3], mis võimaldab E-ITSi rakendajatel oma kaitsealale taotleda rahvusvahelist tunnustamist ISO/IEC 27001 sertifikaadiga.

E-ITSi rakendusjuhend viitab vajadusele sihtobjekte arvele võttes tuvastada etalonturbe kataloogist sihtobjekti puudutavad meetmed [2]. Riigihanke kontekstis tähendab see, et hankija tuvastab enda tellitava IKT-teenusega seotud vajalikud turbemeetmed ning veendub, et meetmed, mida kirjeldatakse hanke tehnilises kirjelduses, on teenust osutades teenuseandja vastutusvaldkonnas.

2.2 Infosüsteemide kolmeastmeline etalonturbe süsteem ISKE

Infosüsteemide kolmeastmeline etalonturbe süsteem, tuntud kui ISKE, kehtis Eestis ajavahemikus oktoober 2003, kui sai valmis esimene rakendusjuhend, kuni 31. detsember 2022. RIA ISKE tutvustuses toodi välja ISKE eesmärk tagada infosüsteemides töödeldavate andmete piisav turvalisus [18]. ISKE rakendusjuhend selgitab, et ISKE oli ette nähtud eelkõige riigi ja kohalike omavalitsuste andmekogude ja nendega seotud infosüsteemide ja infovarade turvalisuse saavutamiseks ja säilitamiseks [19]. ISKE rakendusjuhend kirjeldab ISKE potentsiaalset rakendatavust ka äriettevõtete ja mittetulunduslike organisatsioonide infoturbe eesmärkide saavutamiseks, kuid märgib, et see ei olnud mõeldud riigisaladust käitlevate infosüsteemide turbeks [19]. Vastavalt ISKE määrusele rakendus süsteem andmekogudele, mis viitab sellele, et varem ei vaadeldud organisatsiooni tervikuna [20] .

RIA ISKE-teemalisel veebilehel on kirjeldatud, et nii nagu E-ITSi puhul, oli ka ISKE väljatöötamise aluseks võetud Saksamaa Liitvabariigi BSI avaldatud infoturbe standard IT-Grundschutz [18]. ISKE kolm turbeastet on defineeritud kui madal (L), keskmine (M) ja kõrge (H), mis on ette nähtud andmete turvaklasside määramiseks [18]. Turvaklasside määramise protsess lähtub teabe konfidentsiaalsusese, terviklusese ja käideldavusese hindamisest.

ISKE rakendusjuhendis on kirjeldatud, et muutuv tehnoloogiline keskkond ja uued ohud tingivad etalonturbe meetmestiku regulaarse muutumise ajas, samas märgitakse, et meetmestiku uuendamine sagedamini kui kord aastas ei ole reaalne [19]. Ühtlasi asetas see infoturbe eest vastutajale kohustuse ja vastutuse jälgida järjepidevalt teavet uute ohtude kohta järgmise standardi versiooni ilmumiseni.

RIA koostatud üleminekujuhend ISKE-lt E-ITSile toob kahe süsteemi erinevusena välja, et kui E-ITSi kaitseala määratlemisel lähtutakse kaitset vajavatest äriprotsessidest, siis ISKE puhul oli kaitsealaks andmekogu [21]. Kuigi mõlemad süsteemid põhinevad etalonturbe meetodil, nõuab E-ITS lisaks riskihalduse ja ISMSi juurutamist.

ISKE viimane rakendusjuhend, versioon 8.00, kirjeldab ISKE rakendamise protsessi, mis koosneb järgmistest sammudest [19]:

- infovarade inventuuri ja spetsifitseerimise läbiviimine;
- andmekogude kaardistamine;
- infovarade turvaklassi määramine ja turvaklasside märkimine infovarade spetsifikatsioonidesse;

- kõikide turvaklassiga infovarade vajaliku turbeastme määramine ja nende märkimine infovarade spetsifikatsioonidesse;
- turbeastme M või H korral otsustamine, kas rakendada kogu asutuses ühte turbeastet või jaotada asutus eri turbeastmetega tsoonideks;
- ISKE Portaalist kataloogi B võrdlus infovarade spetsifikatsioonidega ja tüüpmoodulite tähiste märkimine spetsifikatsioonidesse;
- kõrgeimast määratud turbeastmest lähtudes turbehalduse meetmete loetelu koostamine,
- ISKE Portaalist infoturbe halduse mooduli meetmete rakendamise plaani koostamine, muude infovarade turbe rakendamise prioriteetide määramine ja turbe rakendamise plaani tegemine;
- plaani täitmine;
- pärast iga infovara turvameetmete evitamist tegeliku turvaolukorra kontrollimine ISKE Portaalist;
- konfiguratsiooni ja muudatuste halduse käigus hoidmine.

ISKE rakendusjuhend selgitab andmete turvaklasside määramist, sõnades, et andmete turvalisuse tagamise eesmärgid hõlmavad teabe käideldavust (K), terviklust (T) ja konfidentsiaalsust (S), turbetasemete määramiseks kasutatakse neljapallilist skaalat [19]. Neljapallilise skaala abil määratletakse turvaosaklassid, mille tähised koosnevad turvaeesmärgi tähistest ja turvataseme väärtusest, mis võimaldab luua kuni 64 erinevat kombinatsiooni, näiteks K2T3S1 [19]. E-ITSi puhul kasutatakse võrdlusena CIA triaadi. Andmekogu andmeid töötleva infosüsteemi infoturbe eesmärkide tagamiseks on kohustuslik rakendada turvameetmed, mis vastavad selles infosüsteemis peetava andmekogu andmetele määratud turvaklassile [19].

ISKE etalonturbe kataloog, mis on üle 4000 lehekülje pikk, koosneb 15 meetme kataloogist, mida on detailselt kirjeldatud ISKE rakendusjuhendi lisas 1 [22]:

- B1 üldkomponendid;
- B2 infrastruktuur;
- B3 IT-süsteemid;
- B4 võrgud;
- B5 rakendused;
- M1 Infrastruktuur;
- M2 organisatsioon;
- M3 personaal;
- M4 riistvara ja tarkvara;
- M5 side;
- M6 hädaolukorraks valmisolek;
- HG kohustuslikud üldmeetmed;
- HK teabe käideldavuse turvameetmed;
- HT teabe tervikluse turvameetmed;
- HS teabe konfidentsiaalsuse turvameetmed.

Mahukale kataloogile lisandub ohukataloog. Iga moodul sisaldab teema lühikirjeldust, viidates olulistele ohtudele ning soovitatavatele standardsetele turvameetmetele.

ISKE rakendamise keerukust on tajutud mõnda aega enne E-ITSi loomist. Majandus ja Kommunikatsiooniministeeriumi „Küberturvalisuse strateegia 2019–2022" käsitles ISKE rakendamise keerukust, mis oli tuntud probleem enne E-ITSi loomist [23]. Muu hulgas rõhutati, et väikeste kohuslaste, sealhulgas kohalike omavalitsuste hinnangul oli ISKE keerukus ja administratiivne koormus ülejõukäiv ning probleemi tunnetasid lisaks

valitsusasutustele ka väikeettevõtjad, vabakond ja üksikisikud, kes samuti vajasid juhendamist küberriskide haldamisel ning andmekaitse- ja infoturbenõuete täitmisel [23]. Küberturvalisuse strateegia tõi välja vajaduse riikliku toe järele tagamaks baasturbenõuete rakendamise adekvaatsel tasemel. Selleks peeti vajalikuks luua süsteemne ja kergesti kättesaadav abivahendite komplekt, mis hõlmab tööriistu, juhendmaterjale ja koolitusi. Eesmärk oli luua ajakohane, süsteemne ja laialt kasutusel olev baasturbenõuete süsteem, mis integreerib nii infoturbe kui ka andmekaitse miinimumnõuded, et parandada küberturvalisust kõikides ühiskonna sektorites [23]. Sarnaselt E-ITSile on ka ISKE puhul eelduseks juhtkonna kaasatus ja vastutus ning infoturbe ülesannete täitmine on delegeeritud infoturbe spetsialistile.

Alates 2023. aasta algusest on Eestis kehtivaks infoturbe standardiks E-ITS, mis on asendanud eelneva ISKE süsteemi. Sellest hoolimata võib täheldada, et mitmetes riigihangetes esineb endiselt viiteid ISKE standardile, sealhulgas selle turbeklassidele ja -osaklassidele. See näitab, et ISKE mõjutused on endiselt märgatavad hangete tehnilistes kirjeldustes.

2.3 ISO/IEC 27001 Information Security Management System

E-ITSi väljatöötamise üheks eesmärgiks oli saavutada vastavus rahvusvaheliselt tunnustatud ISO/IEC 27001 standardile. See standard määratleb nõuded, millele tuleb vastata ISMSi ülesehitamisel ja haldamisel. ISO/IEC 27001 määratleb juhiseid infoturbe halduse süsteemi loomiseks, juurutamiseks, haldamiseks ja pidevaks täiustamiseks. Standardi auditeerimine on samuti oluline, kuna see võimaldab hinnata süsteemi tõhusust ja tagada selle kooskõla kehtivate nõuetega. E-ITS ja ISO/IEC 27001 jagavad sarnaseid põhimõtteid infoturbe riskide haldamisel ja organisatsiooni kaitsevõime tagamisel: mõlemad standardid rõhutavad riskijuhtimise olulisust ja soosivad pideva täiustamise põhimõtet. Mõlemad standardid nõuavad, et organisatsioonidel oleksid selgelt määratletud turvapoliitikad ja protseduurid ning rõhutavad vajadust määratleda selged rollid ja vastutuse infoturbe juhtimises, nõuavad tehniliste ja korralduslike turvameetmete rakendamist. Regulaarsed sisehindamised ja auditid on mõlema standardi oluline osa, mis aitavad tagada, et turvameetmed vastavad kehtestatud poliitikatele ja eesmärkidele.

Rahvusvaheline Standardiorganisatsioon (ISO) on määratlenud, et standardi ISO/IEC 27001:2022 [24] vastavus tähendab, et organisatsioon on loonud süsteemi haldamaks ettevõttele kuuluvate või hallatavate andmete turvalisusega seotud riske ning süsteem on kooskõlas kõigi rahvusvahelises standardis sätestatud parimate tavade ja põhimõtetega.

Kasvava küberkuritegevuse ja uute tekkivate ohtude kontekstis võib infoturbe riskide juhtimine tunduda keeruline või isegi võimatu [24]. Standardi ISO/IEC 27001 eesmärk on aidata organisatsioonidel saada riskiteadlikuks ning tuvastada nõrkusi ja tegeleda nendega ennetavalt [24]. Sarnaselt E-ITSile lähenetakse infoturbele terviklikult juurutades infoturbe juhtimissüsteem, mis on riskijuhtimise, küberpaidlikkuse ja töökvaliteedi tööriist.

ISO/IEC 27001 standardi Lisa A Turbemeetmed (inglise keeles *controls*), mida täpsemalt käsitletakse dokumendis ISO/IEC 27002:2022, on mõeldud igat tüüpi ja suurusega organisatsioonidele infoturbe riskide käsitlemiseks. Lisa A kontrollide eesmärk on aidata organisatsioonidel määratleda, rakendada, jälgida, üle vaadata ja vajadusel täiendada turvameetmeid vastavalt ISO/IEC 27001 standardi nõuetele, on kirjeldatud ISO/IEC 27002:2022 dokumendi sissejuhatuses [25].

ISO/IEC 27002:2022 veebilehel on kirjeldatud ISO/IEC 27002:2022 standardit, kui täiendavat juhendit, mis keskendub infoturbe kontrollidele (meetmetele), mida organisatsioonid võivad

rakendada [26]. Kuigi ISO/IEC 27001 Lisa A kirjeldab lühidalt iga kontrolli, pakub ISO/IEC 27002 põhjalikumat selgitust, kirjeldab pikemalt iga kontrolli tööpõhimõtet, eesmärki ja pakub parimaid praktikaid, mis on seotud küberturvalisuse aspektidega.

ISO/IEC 27002 standardi sissejuhatus esitab põhielemendid, mille kaudu käsitletakse infoturbe strateegilist lähenemist ja rakendamist organisatsioonides [25]:

- infoturbe nõuded – organisatsiooni vajaduse määratleda oma infoturbe nõuded, nõuded tulenevad kolmest peamisest allikast: a) organisatsiooni riskihindamisest, mis hõlmab võimalike ohtude ja haavatavuste tuvastamist; b) seaduslikest, seadusandlikest, regulatiivsetest ja lepingulistest nõuetest, millele organisatsioon peab vastama; c) organisatsiooni poliitikatest, eesmärkidest ja äritegevusest, mis määravad nõuded infoturbeprotsessidele ja -meetmetele;
- kontrollid – meetmed, mis muudavad või haldavad riske;
- kontrollide määramine – sõltub organisatsiooni otsustest pärast riskihindamist, millel on selgelt määratletud ulatus;
- organisatsioonispetsiifiliste juhendite väljatöötamine;
- seotud rahvusvahelised standardid

Mitmed hankeprotsessis osalevad organisatsioonid on lisanud oma hangete tehnilistesse kirjeldustesse ISO/IEC 27001 vastavuse nõudeid. ISO/IEC 27001 rahvusvaheline tunnustatus ja laialdane rakendamine on teinud sellest eelistatud standardi rahvusvahelistes hangetes, eriti tarkvaraarenduse valdkonnas.

2.4 BSI IT-Grundschutz

BSI (saksa keeles *Bundesamt für Sicherheit in der Informationstechnik*) on Saksamaa Infoturbe Liiduamet. BSI on välja töötanud infoturbe standardi IT-Grundschutz (eesti keeles IT-baaskaitse), mille viimane versioon ilmus 2022. aasta veebruaris [27].

Saksamaa Liitvabariigi riikliku Infoturbe Liiduameti veebilehel on IT-Grundschutz'i kirjeldatud kui usaldusväärset ja jätkusuutlikku infoturbe haldussüsteemi, mis hõlmab võrdselt tehnilisi, organisatsioonilisi, infrastruktuuri ja personali aspekte, pakkudest laiapõhjalist alust infoturbele süstemaatiliseks käsitlemiseks, ühildudes rahvusvahelise standardiga ISO/IEC 27001 [28]. BSI veebilehe kohaselt võimaldab IT-Grundschutz'i edukas rakendamine ettevõttetel või riigiasutustel IT-Grundschutz'i alusel sertifitseerida vastavalt rahvusvaheliselt tunnustatud ISO/IEC 27001 standardile [28].

BSI veebilehel on IT-Grundschutz'i raamistik kirjeldatud kui süsteem, mis koosneb etalonturbe kataloogist ja neljast põhistandardist [28]:
• BSI 200-1 – kirjeldab infoturbe halduse süsteemi ja infoturbe korraldust;
• BSI 200-2 – kirjeldab etalonturbe protsessi, meetmevalikut ja käitust;
• BSI 200-3 – kirjeldab riskihaldust;
• BSI 100-4 – kirjeldab äri jätkuvust.
BSI 200-2-s on kirjeldatud, et IT-Grundschutz'i etalonturbe protseduuri saab kohandada vastavalt eri tüüpi ja suurusega organisatsioonide nõuetele [28]. Seda rakendatakse kolme metoodika kaudu: standard-, põhi- ja tuumikkaitse. Metoodika on kavandatud pakkuma asjakohast kaitset organisatsiooni teabe haldamiseks. BSI poolt pidevalt arendatud metoodika pakub endast väärtuslikku ressurssi organisatsioonidele: juhised ISMSi loomiseks ja igakülgse riskianalüüsi alust, olemasoleva turbetaseme hinnangut ja asjakohase infoturbe taseme rakendamist.

BSI IT-Grundschutz'i metoodika dokumendis on välja toodud, et BSI avaldab IT-Grundschutz'ile lisaks erinevaid metoodikaid, mis on kohandatud tüüpiliste äriprotsesside ja rakenduste turvameetmetele, mida vastavalt vajadusele organisatsioonis juurutada, need hõlmavad turvameetmeid süsteemidele, andmesidele ja ruumidele [29].

BSI IT-Grundschutz'i metoodikas on eraldi välja toodud, et organisatsiooniliste, personali-, infrastruktuuri- ja tehniliste turvameetmete rakendamisel on võimalik saavutada standardkaitse, mis tagab äriprotsesside ja ettevõtlusega seotud teabe kaalutletud turvalisuse taseme [29]. Põhikaitse rakendamine saavutab turvalisuse taseme, mis on standardkaitsest oluliselt madalam, pakudes siiski tugevat alust ISMS-i loomiseks. Tuumikkaitsemeetodit saab kasutada teabe ja äritegevuse protsesside kaitsmiseks, mis nõuavad kõrgendatud kaitset.

IT-Grundschutz'i moodulid on kategoriseeritud fookuse alusel protsessi- ja süsteemimooduliteks ning rühmitatud teemade sobitamise alusel. Protsessimoodulid sisalduvad järgmistes kihtides:
• ISMS – infoturbe haldussüsteemid
• ORP – organisatsioon ja personal
• CON – kontseptsioonid
• OPS – käidutööd
• DER – tuvastus ja reaktsioon
Süsteemimoodulid on rühmitatud järgmistesse kihtidesse:
• INF – infrastruktuur
• NET – võrgud ja side
• SYS – IT-süsteemid
• APP – rakendused
• IND – tööstuslik IT
Iga moodul pakub teema lühikirjeldust ja selgitab saavutatavat eesmärki, samuti pakutakse ülevaadet käsitletava teema spetsiifilistest riskidest, et tagada nende mõistmine ja haldamine vastavalt määratud kaitsetasemele [29].

Sarnaselt IT-Grundschutz'ile rakendab E-ITS moodulite struktureerimist kaitsetaseme põhjal, jagades moodulid protsessi- ja süsteemimooduliteks ning grupeerides moodulid samade teemade alusel. Selline lähenemine näitab IT-Grundschutz'i olulist mõju E-ITSile.

3. Seadused ja määrused seoses E-ITSi ja riigihangetega

Käesolev peatükk kirjeldab seadusandlikke raamistikke ja regulatiivseid nõudeid, mis on olulised nii riigihanke, kui ka E-ITSi kontekstis. RIA küberturvalisuse 2022. aastat kirjeldava aastaraamatu artiklis „E-ITS: miks ja kellele" [9] on kirjeldatud, et Küberturvalisuse seaduse muudatustest tulenevalt on ligikaudu 3500 organisatsioonil kohustus järgida antud standardit. E-ITSi rakendamise kohustuslike subjektide kohta pakub detailsemaid selgitusi Küberturvalisuse seadus, tuntud kui KüTS, tuues ühtlasi välja teenuse osutaja kohustuse tagada, et kolmas osapool, kes organisatsiooni süsteemi haldab, rakendab asjakohaseid turvameetmeid. Hädaolukorra seadus määratleb omakorda, mis kujutab endast elutähtis teenus ning seab samuti kohustuse tagada elutähtsate teenuste osutajate poolt kasutatavate võrgu- ja infosüsteemi elektrooniline turvalisus. Hetkel on mitmed elutähtsate teenusete osutajad hanke korras IKT teenuseid tellimas. Võrgu- ja infosüsteemide küberturvalisuse nõuded hõlmavad turvameetmete üldnõudeid ja süsteemide turvameetmete erinõudeid ning nende kohaldamise ulatust, mis laieneb paljudele hankeid läbiviivatele organisatsioonidele. Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel sätestab reeglistiku ja juhised avaliku sektori asutustele, kes kasutavad pilvandmetöötlusressursse avaliku teabe töötlemiseks. Riigihangete seadus esitab juhised ja nõuded riigihangete läbiviimiseks.

3.1 Eesti infoturbestandard

Eesti infoturbestandardi määrus, kehtestatud küberturvalisuse seaduse paragrahv seitse lõike viis ning Vabariigi Valitsuse 9. detsembri 2022. aasta määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded" paragrahv kolm lõike üks alusel, määratleb, et teenusepakkujad peavad tagama võrgu- ja infosüsteemide turvalisuse, järgides Eesti infoturbestandardit ja rakendades sellega seotud turvameetmeid [12]. Samuti kohustab määrus teenusepakkujaid järgima E-ITSi põhimõtteid infoturbe halduse eri etappides, sealhulgas käivitamisel, rakendamisel, käigushoidmisel ja täiustamisel. Lisaks nõuab Eesti infoturbestandardi määrus E-ITSi tingimuste täitmise auditeerimist, et tagada standardi nõuetekohane rakendamine.

3.2 Küberturvalisuse seadus

Küberturvalisuse seadus, vastu võetud 9. mail 2018, on õigusakt, mis on loodud reguleerima ühiskonna toimimise seisukohast oluliste võrgu- ja infosüsteemide pidamise nõudeid, vastutust ja järelevalvet ning küberintsidentide ennetamise ja lahendamise põhimõtteid [4]. E-ITSi kontekstis määratleb see seadus asutused ja organisatsioonid, mille jaoks on E-ITSi rakendamine on kohustuslik.

Küberturvalisuse seaduse (KüTS) kohaselt kvalifitseeruvad elutähtsa teenuse osutajateks mitmed organisatsioonid ja ettevõtted, kelle tegevus on oluline ühiskonna toimimiseks [4]. Nende hulka kuuluvad raudtee-ettevõtjad, lennuväljade käitajad, sadamateenuse osutajad, suuremahuliste sideettevõtjate kaabelleviteenuse osutajad, tervishoiuteenuste osutajad, perearstid, tipptaseme domeeninimede registri haldajad, kriitilise tähtsusega side- ja mereraadioside teenuse osutajad, ning Eesti Rahvusringhääling. Lisaks nendele peavad seaduse nõudeid järgima ka andmekogude vastutavad ja volitatud töötlejad, finantsasutused nagu Eesti Pank, õigus- ja haldusasutused, kohaliku omavalitsuse üksused ning mitmed teised riigi ja avalik-õiguslikud juriidilised isikud.

Küberturvalisuse seaduse paragrahv kuus selgitab küberturbe tagamise põhimõtteid järgmiselt [4]:

- isiklikkuse põhimõte: süsteemi turvalisuse eest vastutab teenuse osutaja;
- tervikliku kaitse põhimõte: teenuse osutaja tuvastab võimalikud ohud süsteemile ja rakendab süsteemi kaitsmiseks sobivaid korralduslikke ja tehnilisi meetmeid;
- kahjuliku mõju vähendamise põhimõte: küberintsidenti korral rakendab teenuse osutaja vajalikku hoolsust ja meetmeid, et piirata küberintsidenti põhjustatud kahju laienemist teistele süsteemidele. Samuti teavitab ta küberintsidendist seaduses määratletud järelevalveasutust;
- koostööpõhimõte: küberturvalisuse tagamisel ja küberintsidentide lahendamisel osalevad asjaosalised koostöös, võttes vajaduse korral arvesse süsteemide ja teenuste omavahelist seotust ning sõltuvust.

Küberturvalisuse seaduse paragrahv seitse kehtestab teenuse osutajatele mitmeid kohustusi, mis on suunatud küberturvalisuse tõhustamisele. Need hõlmavad järgmisi tegevusi [4]:

- riskianalüüsi koostamine: teenuse osutaja peab looma süsteemi riskianalüüsi, mis sisaldab ohtude loetelu, nende mõjude hindamist, küberintsidendi tagajärgede raskusastet ning nende lahendamiseks vajalikke abinõusid;
- riskianalüüsi dokumenteerimine: süsteemi riskianalüüsi, turvaeeskirju ja turvameetmete rakendamise kirjeldusi on kohustuslik hoida ajakohastatud ning kättesaadavana;
- süsteemi seire: teenuse osutaja peab jälgima süsteemi, et tuvastada ohustavad tegevused või tarkvara, ja informeerima sellest RIAt;
- küberintsidendi mõju ja leviku piiramine: vajadusel tuleb rakendada abinõusid, mis aitavad vähendada küberintsidendi mõju ja takistada selle levikut, sealhulgas piirata süsteemi kasutamist või juurdepääsu süsteemile.

KüTS käsitleb olukorda, kus teenuse osutaja kasutab välise teenuseandja teenuseid või delegeerib süsteemi haldamise kolmandale osapoolele. Seadus nõuab, et teenuse osutaja peab tagama, et kolmas osapool, kes süsteemi haldab, rakendab asjakohaseid turvameetmeid. Selle sätte alusel jääb esmane vastutus süsteemi turvalisuse eest teenuse osutajale, sõltumata, kas süsteemi haldab teenuse osutaja ise või volitatud väline isik [4].

KüTSi teises peatükis, mis keskendub „Kohustustele küberturvalisuse tagamiseks", on määratletud mitmed turvameetmed, mida teenuse osutajad peavad rakendama. Paragrahv seitse, punkt viis sätestab süsteemide turvalisuse tagamiseks järgmised kohustused: esiteks infoturbe halduse nõuded, mis on üldnimetatud Eesti infoturbestandardiga; teiseks turvameetmete üldnõuded; ja kolmandaks süsteemide turvameetmete erinõuded koos nende kohaldamise ulatusega [4].

3.3 Hädaolukorra seadus

Hädaolukorra seadus moodustab õigusliku raamistiku erakorraliste olukordade haldamiseks, mis kujutavad endast potentsiaalset ohtu inimeste elule, tervisele, varale või keskkonnale [30]. Seadus sätestab ennetavad, valmistumis-, lahendus- ja järelmeetmed hädaolukordadeks, eesmärgiga leevendada nende mõju. Samuti identifitseerib ja määratleb see elutähtsate teenuste osutajad, pannes neile konkreetsed kohustused hädaolukordades toimimise tagamiseks. Küberturvalisuse seadus on defineerinud elutähtsa teenuse osutajad, kellele on E-ITSi rakendamise kohustus.

Järgnevas lõigus määratleb Hädaolukorra seadus „elutähtsa teenuse" kui teenuse, mis avaldab märkimisväärset mõju ühiskonna toimimisele ja mille katkemine kujutab endast otseseid riske inimeste elule või tervisele või ohustab teise elutähtsa teenuse toimimist. Elutähtsate teenuse hulka kuuluvad teenused koos nende toimimiseks vajalike ehitiste, seadmete, personali ja varudega. Elutähtsa teenuse toimepidevus viitab teenuse osutaja võimele säilitada järjepidev toimimine ning taastada normaalne toimimine pärast teenuse katkestust [30].

Peatükk viis Hädaolukorra seadusest käsitleb elutähtsate teenuste toimepidavuse korraldust, mille paragrahv 41 toonitab elutähtsa teenuse osutajate kohustust tagada nende poolt kasutatavate võrgu- ja infosüsteemi elektrooniline turvalisus, järgides Küberturvalisuse seaduse paragrahve seitse ja kaheksa ning nende alusel kehtestatud nõudeid [33].

3.4 Võrgu- ja infosüsteemide küberturvalisuse nõuded

Võrgu- ja infosüsteemide küberturvalisuse nõuete määrus, mis on vastu võetud 09.12.2022, on kehtestatud küberturvalisuse seaduse paragrahv seitse lõike viis alusel [13]. Sellega on antud üleriigilise küberturvalisuse tagamise eest vastutavale ministrile volitus kehtestada Eesti infoturbestandard, mis hõlmab turvameetmete üldnõudeid ning süsteemide turvameetmete erinõuded ja nende kohaldamise ulatust. Võrgu- ja infosüsteemide küberturvalisuse nõuete määrus kirjeldab Eesti infoturbestandardi kehtestamise protsessi ja kohaldamise erandid. Konkreetsete erandite alusel on teatud teenuse osutajad vabastatud E-ITSi nõuete rakendamisest, kui nad vastavad kahele kriteeriumile: esiteks, nende rakendatud turvameetmed peavad vastama rahvusvahelisele standardile ISO/IEC 2700 ning nad peavad esitama RIA-le kehtiva vastavussertifikaadi, mis tõendab ISO/IEC 27001 nõuete täitmist; teiseks on sätestatud erandid julgeolekuasutustele, millele ei kohaldata E-ITSi nõudeid juhul, kui nad vastavad eelnimetatud ISO/IEC 27001 standardi nõuetele ja esitavad nõutud vastavussertifikaadi küberturvalisuse seaduse alusel määratud haldusjärelevalve teostajale.

Võrgu- ja infosüsteemide küberturvalisuse nõuete määruse kolmandas peatükis adresseeritakse turvameetmete üldnõudeid ja erinõudeid andmekogudele. Esimene jagu käsitleb süsteemide kaardistamist, dokumenteerimist ja riskianalüüsi. Teine jagu, erinõudeid, mis käsitleb konkreetsemalt andmekogude pidamise turvameetmeid, kattub ISKE raamistikus seatud nõuetega andmekogudele. Selles jaoks käsitletakse andmekogu turbeastme määramist, mis võib olla kõrge (H), keskmine (M) või madal (L), ning andmete turvaklassi määramist, mis hõlmab käideldavuse, tervikluse ja konfidentsiaalsuse parameetrite kombinatsiooni, näiteks K2T3S1. Lisaks kirjeldatakse, kuidas määratakse andmete turvaosaklassid ja rakendatakse turvameetmeid vastavalt andmekogu määratud turbeastmele [13].

Paragrahv 11 Võrgu- ja infosüsteemide küberturvalisuse nõuete määrus kirjeldab lisaks, kuidas tuleb turvameetmeid rakendada sõltuvalt andmekogu turbeastmest [13]. Andmekogu vastutav töötleja ja majutav volitatud töötleja peavad tagama, et kõik andmekoguga seotud süsteemid ja teenused vastavad määratud turbeastmele. See tähendab, et turbeastme määratlusest tulenevalt peavad olema paika pandud ja rakendatud asjakohased turvameetmed, mis hõlmavad kaitsetarvet vastavalt Eesti infoturbestandardile: kõrgele turbeastmele (H) vastab väga suur kaitsetarve (VS), keskmisele (M) suur kaitsetarve (S) ja madalale (L) normaalne kaitsetarve (N).

Teine jaotis Võrgu- ja infosüsteemide küberturvalisuse nõuete määruses identifitseerib süsteeme, mis oluliselt mõjutavad riigi ja kohaliku omavalitsuse üksuste võimet täita avalikke ülesandeid [13]. Nimetatud süsteemid peavad järgima kindlaid turvanõudeid, mille hulka kuulub nende tarkvara lähtekoodi, andmete ja taastejuhendite regulaarne varundamine

turvalisse andmekeskusesse, mis asub välisriigis ja mille tegevus põhineb rahvusvahelisel lepingul.

Neljas peatükk Võrgu- ja infosüsteemide küberturvalisuse nõuete määruses käsitleb Eesti infoturbestandardile ülemineku rakendussätteid – kuni 31. detsembrini 2022 eeldati, et teenuse osutajad, kes haldavad riigi või kohaliku omavalitsuse üksuste süsteeme, rakendavad nõuetekohaseid turvameetmeid vastavalt kehtestatud määrustele. Seejärel, kuni 30. juunini 2023, kehtis sama ootus ka neile teenuse osutajatele, kes neid süsteeme ei halda, eeldusel, et nad järgivad aktiivselt Eesti infoturbestandardit ja seiravad süsteemide turvalisust hõlmavaid turvameetmeid [13].

3.5 Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel

Määrus Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel (tuntud kui Pilvemäärus) on vastu võetud 03. jaanuaril 2024, see sätestab reeglistiku ja juhised avaliku sektori asutustele ning teistele määruses defineeritud isikutele, kes kasutavad pilvandmetöötlusressursse avaliku teabe töötlemiseks. Määrus kehtestatakse avaliku teabe seaduse ja küberturvalisuse seaduse alusel [31].

Paragrahvis üks Pilvemääruses on välja toodud juhud, millal määrust kohaldatakse: määrus rakendub juhul, kui teabepidaja kasutab avaliku teabe töötlemiseks avaliku sektori osutatavat pilvteenust või muid pilvandmetöötlusteenuseid [31]. Lisaks sätestatakse, et kui teabepidaja delegeerib avaliku ülesande täitmise teisele asutusele või isikule, jääb algne teabepidaja vastutavaks määruse nõuete täitmise eest.

Paragrahv kaks Pilvemäärusest sätestab protseduurid ja nõuded, mida teabepidajad peavad järgima enne pilvteenuste kasutuselevõttu avaliku teabe töötlemisel [31]. Teabepidaja on kohustatud läbi viima põhjaliku hindamise, mis hõlmab järgmisi aspekte: avaliku teabe olemus, sellega seotud riskid, nõuded teabe tervikluse, käideldavuse ja konfidentsiaalsuse tagamiseks, pilvteenuse pakkuja usaldusväärsus ja nõuetele vastavus, kasutatava tehnoloogia mõju olemasolevale süsteemile ning pilvteenuse turvalisus. Lisaks on võimalik arvesse võtta olemasolevaid auditeid ja rahvusvaheliselt tunnustatud sertifikaate. Hindamisprotsessi dokumenteerimine on kohustuslik ja see võib toimuda osana laiemast õigusaktiga reguleeritud dokumentatsioonist.

Paragrahv kolm Pilvemäärusest esitab nõuded ja protseduurid, mida teabepidajad peavad enne avaliku teabe töötlemiseks pilvteenuste kasutuselevõttu järgima [31]. Teabepidajad on kohustatud määratlema avaliku teabe käideldavuse, tervikluse ja konfidentsiaalsuse nõuded ning sätestama pilvteenuse pakkuja suhtes kohaldatavad tingimused, sealhulgas juurdepääsuõigused ja küberintsidentide teavitamise kord. Lisaks peavad nad kindlaks määrama teabe seiratavuse ja töötlemistoimingute tuvastamise meetodid ning määratlema pilvteenuse kasutamise ja avaliku teabe töötlemise lõpetamise tingimused, kaasa arvatud andmete arhiveerimise ja kustutamise kohustused. Kõik teabepidaja ja pilvteenuse pakkuja vahelised õigused ja kohustused on vaja kirjalikult fikseerida. Teabepidaja peab viivitamata teavitama RIA-t või vastavaid järelevalveasutusi pilvteenuse kasutuselevõtust, esitades teavet pilvteenuse pakkuja, kasutuse ulatuse ja konteksti kohta. Erandid teavitamisele on ette nähtud juhul, kui pilvteenust kasutatakse ühekordseks avaliku ülesande toetamiseks või kui pilvteenust ei ole määruse kohaselt hinnatud.

Paragrahvid neli kuni kuus määrusest reguleerivad pilvteenuste kasutamise jälgimist, lõpetamist ja määruse rakendamise ajakava, et tagada avaliku teabe töötlemise turvalisus pilvkeskkonnas [31]. Paragrahv neli kohustab teabepidaja jälgima avaliku teabe käideldavuse, tervikluse ja konfidentsiaalsuse nõuete täitmist ning hindama pilvteenuse tingimuste muutuste mõju. Paragrahv viis käsitleb pilvteenuse kasutamise lõpetamist, nõudes töödeldud avaliku teabe kustutamist viisil, mis välistab andmete taastamise või edasise töötlemise. Samuti nõuavad mõlemad paragrahvid viivitamatut teavitamist RIA-le või vastavale järelevalveasutusele muudatuste, k.a teenuse kasutamise lõpetamise korral.

3.6 Riigihangete seadus

Riigihangete korraldamine on reguleeritud Riigihangete seadusega, mis võeti vastu 14.06.2017, esitades juhised ja nõuded riigihangete läbiviimiseks [32]. Paragrahv kaheksa käsitleb hankelepingut, mis on defineeritud kui lepinguline kokkulepe hankija ja ettevõtja vahel ning hõlmab rahaliste huvidega seotud tehinguid seoses asjade, teenuste või ehitustöödega. Hankelepingule kohalduvad kehtestatud korrad ning see peab olema sõlmitud kirjalikus vormis, kui selle maksumus ületab 20 000 eurot, välja arvatud juhul, kui riigihanke alusdokumentides on sätestatud teisiti.

Riigihangete seaduse kohaselt algab hankemenetlus hanketeate avaldamisega registris, erandina väljakuulutamiseta läbirääkimistega hankemenetlus, mis algab läbirääkimiste ettepanekuga valitud ettevõtjatele [32]. Hankemenetlus võib lõppeda hankelepingu sõlmimisega, pakkumuste tagasilükkamisega, kõigi pakkujate kõrvaldamisega või hankemenetluse kehtetuks tunnistamisega.

Samuti määrab riigihangete seadus alusdokumentide elektroonilise kättesaadavuse ja vajalikku teave sisaldavuse seoses hankelepingu tingimuste ja menetlusega [32]. Hankemenetluse alusdokumentide hulka peavad kuuluma hankelepingu tehniline kirjeldus, hindamiskriteeriumid, alternatiivsete lahenduste nõuded, tingimused võistlevate pakkumuste saamiseks ning muu oluline teave, mis mõjutab pakkumuste esitamist ja hindamist. Hanketeates esitatud teave on kõige olulisem ja seda peetakse ülimuslikuks muu teabe suhtes.

Riigihangete seaduse tehnilise kirjelduse jaotis sisaldab teavet tehnilise kirjelduse kohta, mis hõlmab hankelepingu eseme omaduste ja nõuete loetelu, mis on esitatud vastava eriala spetsialistidele selges ja arusaadavas terminoloogias [32] Tehnilise kirjelduse koostamisel on hankijal lubatud kasutada Euroopa standardeid või teisi tehnilisi kontrollisüsteeme, tagades, et kirjeldus ei soosi ühtegi ettevõtjat või toodet, tagamaks võrdsed konkurentsitingimused kõigile osalejatele.

Riigihangete seaduse viies jaotis on pühendatud hankelepingu sõlmimise ja täitmise korraldusele [32]. Hankelepingu sõlmimine toimub vastavalt riigihanke alusdokumentides määratletud tingimustele ja aluseks on edukaks tunnistatud pakkumus, mis vastab hankija poolt kehtestatud nõudele ja kriteeriumitele. Hankelepingut võib jagada osadeks ning iga osa jaoks võib sõlmida eraldi lepingu. Hankeleping on tühistatav, kui hankija rikub seaduses sätestatud nõudeid.

4. Riigihangete korraldamine

Krisi Pungas on oma uurimuslikus artiklis, mis avaldati 14. detsembril 2016 nõustamisteenuseid pakkuva ettevõtte Grant Thornton Baltic OÜ veebilehel, esitlenud riigihanke protsessi kuut etappi. Artiklis pealkirjaga „Riigihangetega seotud protsessid organisatsioonis" annab Pungas etapiliselt ülevaate kogu hanke protsessist ning selgitab kuidas need etapid mõjutavad organisatsiooni üldist tegevust [33].

Artiklis käsitletakse esimese punktina hankevajaduse määratlemist [33]. Hankevajaduse määramine hõlmab hanke ajalist määratlust ja sisaldab hanke planeerimist. Planeerimise käigus koostatakse hankedokumendid, mis sisaldavad sealhulgas hangitava objekti tehnilist kirjeldust. Selles etapis moodustatakse riigihanke komisjon, mis koosneb organisatsiooni liikmetest, kes vastutavad hanke elluviimise eest. Hankevajaduse määratlemisel ja hanke planeerimisel on kõige olulisem sisend isikutelt, kes hakkavad hangitavat objekti kasutama. Nende panus on eriti oluline tehnilise kirjelduse koostamisel ning pakkujate kvalifikatsiooninõuete ja pakkumuste hindamiskriteeriumide seadmisel. Nende valdkondlikud teadmised tagavad, et hangitava eseme kirjeldus ja hindamiskriteeriumid vastaksid tarbijate vajadustele.

Järgnevas etapis, mida Pungas kirjeldab kui läbiviimise faasi, on hanke protsessis menetlust korraldavatel spetsialistidel kõige aktiivsem roll [33]. Selles faasis viiakse läbi riigihangete seadusest ja asutuse sisekorrast lähtuvad kohustuslikud menetluslikud tegevused, nende hulka kuuluvad hanketeate avaldamine, pakkumuste vastuvõtmine, pakkujate ja pakkumuste hindamine, hindamise dokumenteerimine, eduka pakkuja valimine, otsuste tegemine, suhtlemine pakkujatega, lepingute sõlmimine ning riigihanke aruande esitamine.

Peale hankemenetluse läbiviimist ja lepingu sõlmimist toimub kauba tarnimine või teenuse osutamine. Selles protsessis osalevad lõpptarbijad, kes tajuvad hanke planeerimise tulemusi. Lõppkasutajate kogemused ja rahulolu on otseselt mõjutatud sellest, kui kvaliteetselt oli planeerimine teostatud ning kuivõrd aktiivselt osalesid nad tehnilise kirjelduse koostamisel.

Pungas kirjeldab viimase etapina tasumist ja aruandlust, mis järgneb kauba või teenuse kättesaamisele [33]. Riigihangetega seotud protsessi lõpetab aruandlus, mida tuleb esitada mitmel suunal. Esiteks tuleb esitada riigihangete registrile riigihanke aruanne, kus kajastatakse hankeobjekti eest tasutud tegelikult maksed. Lisaks tuleb esitada aruanne organisatsiooni juhtkonnale, mis võib olla kas ühekordne teavitus konkreetse hanke lõpetamise kohta või regulaarne, mille esitamise sagedus sõltub organisatsiooni suurusest ja vajadustest. Aruandlus mängib olulist rolli juhtimisotsuste tegemisel ning riskide maandamisel, võimaldades adekvaatselt reageerida probleemidele ning tagada organisatsiooni põhiülesannete tõrgeteta täitmine.

5. Riigihangete analüüs

Järgnev peatükk keskendub sellele, kuidas hankijad on spetsifitseerinud oma IKT-teenuste turvanõuded ja millisel määral saavad teenuseandjad neile vastata. Analüüs põhineb 2023. aastal väljastatud hankedokumentidel. Autor keskendub detailsemalt kahele hankele: „KEMIT Postgre andmebaasi majutusteenus 2024–2028" ja „Infosüsteemide majutusteenuse tellimine ETIS ja EHIS". Näited on valitud nende esinduslikkuse tõttu, kuna illustreerivad teenuseandjate ees seisvaid keerukusi hankepakkumiste koostamisel.

Autor analüüsis hangete kirjelduses toodud turvameetmeid ning kategoriseeris need meetme täitmise eest vastutava alusel kolme rühma:

- meetmed, mida teostab üksnes hankija – turvapoliitikad ja protseduurid, mis on määratletud hankija organisatsioonisiseste regulatsioonidena ja mille eest hankija vastutab;
- meetmed, mida teostab teenuseandja – hõlmavad tehnilisi ja operatiivseid turvameetmeid, mis on seotud andmete majutamise ja haldamisega, ning mille rakendamine on otseselt teenuseandja kohustus;
- meetmed, mille eest vastutus on ühiselt jaotunud – koostööl põhinevad meetmed, nagu ühised turvaauditid ja riskihindamised, mis nõuavad mõlema poole aktiivset osalust ja vastutust.

Hinnang põhineb autori isiklikel kogemustel ja vaatlustel, pakkudes hinnanguid turvameetmete adekvaatsusele ja nende rakendamise vastavusele hanke nõuetega.

5.1 Näited riigihangete turvameetmete tehnilistest kirjeldustest 2023. aastal

Järgnevas osas on toodud konkreetsed näited riigihangete tehnilises kirjelduses esitatud turvameetmete nõuetest, eesmärgiga illustreerida magistritöö kontekstuaalset relevantsust. Näited sisaldavad viiteid juba kehtivuse lõppenud ISKE-le, hangetele, kus kirjeldused on üldsõnalised, jättes palju tõlgendamisruumi, või kus „ISKE" on vahetatud „E-ITSi" vastu.

5.1.1 IKT-halduse teenus Türi Vallavalitsusele

IKT-halduse teenus Türi Vallavalitsusele hankes telliti hankijale 36 kuuks IKT-halduse teenust, mis sisaldas IT-vahendite haldusteenust, serveriteenust, tark- ja riistvarahalduse tööriista kasutamise teenust ja kõiki teenuse käivitamise, üleval hoidmise, lõpetamise ning üleandmisega seotud tegevusi [34].

Serverteenuste üldnõuete all olid toodud järgnevad nõuded:
„Lepingu perioodil peab pakkuja tagama serveriteenuse turvalisuse (käideldavus K2, terviklikkus T1, turvalisus S2, rakendab vähemalt ISKE keskmise turbeastme meetmeid), sealhulgas tegema kõik turvalisuse tagamiseks vajalikud uuendused, seadistused jms;
Serveriteenuse pakkumisel kasutatavad serveriruumid peavad vastama ISO 27001 infoturbe juhtimissüsteemi standardile."

Autori hinnangul on nõuded üldsõnalised, viide ISKE-le ei ole enam hanke väljastamise ajal relevantne. Samuti ei ole ISKE meetmed üks-ühele üle kantavad E-ITSi meetmeteks.

5.1.2 Turbekeskus teenusena

Turbekeskus teenusena hankes telliti Ettevõtluse ja Innovatsiooni Sihtasutusele kuutasu põhiselt kuni 48 kuulise ajaperioodi jooksul turbehalduskeskuse teenust (inglise keeles *Security*

Operation Center as a Service, SoCaaS) Microsoft Sentinel SIEM (inglise keeles *Security Information and Event Management*) baasil [35].

Hangitava teenuse üldnõuete all oli toodud järgnevad nõuded:
„Turbekeskuse teenuse korraldus peab lähtuma rahvusvahelise standardi ISO/IEC 27001 ja Eesti infoturbestandardi (E-ITS) nõuetest teenuse osutamisel."

Autori hinnangul on nõuete kirjeldus üldsõnaline ja jätab palju tõlgendamisruumi, millised on nõuded, millele oodatakse vastamist. Jääb ebaselgeks, kas soovitakse mõlemale standardile vastamist või on teenuseandjal valik.

5.1.3 Tallinna sporditegevuse toetuste infosüsteemi arendus-, hooldus- ja majutusteenus

Tallinna sporditegevuse toetuste infosüsteemi teenuse hankes telliti infosüsteemi arendus-, hooldus- ja majutusteenust [36].

Hangitava teenuse süsteemi kirjelduses oli toodud järgmine info:
„Infosüsteemi turvaklass on K2T2S2 ja turbeaste on M (keskmine). Pakkuja peab pakkumuse tegemisel ja teenuse osutamisel arvestama vastava turbeastmega süsteemide standardseid turvameetmeid tulenevalt Vabariigi Valitsuse 9. detsembri 2022 määrusest nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded" ja Ettevõtlus- ja infotehnoloogiaministri määruse 24.12.2022 (RT I, 21.12.2022, 34) „Eesti infoturbestandard". Infosüsteemile tuleb rakendada E-ITS standardturve turbeviisi meetmeid."

Autori hinnangul jätab nõuete kirjeldus palju tõlgendamisruumi. Hankija ootus jääb ebaselgeks, milliste meetmete rakendamist millistele komponentidele oodatakse. Samuti on hankes kuvatud turvaklassid, mis ei ole E-ITSi raames relevantsed.

5.1.4 Juhtimistarkvara kasutusõiguse teenuse tellimine

Juhtimistarkvara kasutusõiguse teenuse tellimise hankes telliti Pärnu Linnavalitusele planeerimise, projektijuhtimise ja personalihindamise keskkond [37].

Hangitava teenuse kirjelduses oli kvaliteedi- ja turvanõuete alltoodud hankija järgmised soovid:
„Infosüsteemide kolmeastmeline etalonturbe süsteemi (ISKE) turvaklass Infosüsteemil on K2T1S1. Pakkuja peab rakendama kõiki asjakohaseid ISKE M taseme meetmeid Infosüsteemi piires."
„Tarkvara peab vastama OWASP (Open Web Application Security Project) rakenduste turvanõuete standardi ASVS (Application Security Verification Standard) versiooni 4.0.3 Level 2 või kõrgema taseme nõuetele."

Autori hinnangul on nõuete kirjeldus üldsõnaline ja jätab palju tõlgendamisruumi. Hankija ootus jääb ebaselgeks, mis on hankija jaoks asjakohased meetmed. Samuti oli hanke väljastamise ajal käibel E-ITS.

5.1.5 Andmesideteenus Tallinna hallatavatele asutustele

Andmesideteenus Tallinna hallatavatele asutustele hankes telliti andmesideteenus, mis sisaldas laivõrguteenust, internetiühenduse teenust, tulemüüriteenust, VPN teenust, Wi-Fi pääsupunktide renti ja haldust, sisevõrgu haldusteenust, monitooringut, kasutajatuge ja aruandlust [38].

Hangitava teenuse üldkirjelduses oli toodud meetmena:
„Teenusele tuleb rakendada E-ITS (https://eits.ria.ee/, https://www.riigiteataja.ee/akt/121122022034) standardturve turbeviisi meetmeid."

Autori hinnangul jätab nõuete kirjeldus palju tõlgendamisruumi. Hankija ootus jääb ebaselgeks, kas hankija soovib, et teenuseandja oleks kõikide E-ITSi standardmeetmete rakendaja hankes nimetatud teenuste puhul, kaasa arvatud organisatsioonisiseste tegevuste täitmist.

5.1.6 Majutus- ja administreerimisteenus[1]

„Serveriruumid peavad olema spetsiaalselt ehitatud serverite majutuseks ja vastama E-ITS turbeastmele H ning standardile ANSI/TIA-942 (Telecommunications Infrastructure Standard for Data Centers) tasemele Tier 3, mööndusega, et varugeneraator ei pea olema dubleeritud."

Autori hinnangul ei saa teenuseandja vastata hankenõuetele, kuna E-ITSis puudub vastav turbeaste.

5.2 Riigihange „KEMIT Postgre andmebaasi majutusteenus 2024–2028"

KEMIT Postgre andmebaasi majutusteenus 2024–2028 hankedokument kirjeldab hankija hetkeolukorda ja vajadusi PostgreSQL andmebaaside majutamise ja haldamise teenust hankides [39]. Hange on valitud autori poolt vaatlusaluseks, kuna sisaldab tehnilises kirjelduses E-ITSi mooduleid, mille täitmist oodatakse teenuseandja käest täies mahus. Autor võrdsustab meetmete kirjelduse sarnaseks 5.1.5 punktid toodud näitega, kus teenuseandjalt oodatakse ka organisatsioonisiseste tegevuste täitmist.

5.2.1 Hanke ülevaade

Hankija tunnistab oma piiratud kompetentsi PostgreSQLi haldamisel, mis on andnud aluse vajadusele majutada osaliselt baasid teenuseandja juurde, kasutades teenuseandja kompetentse halduse osas. Dokumendis on esitatud kvantitatiivsed detailid, mis kajastavad hankija umbes 250 PostgreSQL andmebaasi. Lisaks on määratletud soovitud teenusekäideldavuse nõuded (SLA) ja ressursinõuded ning eeldatav andmebaaside haldamise aeg kuus.

KEMIT Postgre andmebaasi majutusteenus 2024–2028 hankedokumendis on üldnõuete osas sätestatud, et teenuseandja on kohustatud rakendama ISO/E-ITS samas käsitlusalas, mille raames teenust hangitakse [39]. On lisatud, et pakutav teenus peab vastama hanke dokumendis eraldi välja toodud E-ITSi põhi- ja standardmeetmetele. Samuti peab teenuseandja tagama teenuse turvalisuse ja ajakohasuse.

Majutusteenuse hankedokumendis on rõhutatud, et hankija soovib juurkasutaja õiguseid ja kontrolli oma andmebaaside üle, teenuse nõuded juurkasutaja (ingl keeles *Superuser*) vaates välistavad teenuseandja täiskontrolli [39].

Hankija soovitud teenuse – PostgreSQL andmebaaside majutuse ja halduse – kontekstis ei pruugi kõik hankes mainitud E-ITSi moodulid olla võrdselt olulised või vajalikud. Hankes mainitud moodulid on: Taristu (INF.1; 2, 5, 6, 12, 13), Võrk (NET.1.1, 1.2, 3.1, 3.2). Server (SYS 1.1, 1.2, 1.3, 1.5, 1.6, 1.8), Klientarvuti (SYS.2.1, 2.2, 2.3, 2.4), Rakendused ja

[1] Väljakuulutamiseta läbirääkimistega menetlus

andmebaasid (APP.4.3), Infoturve ja andmevahetus (CON.2, 3), Õiguste haldus ja ligipääsud (ORP.4) ja Andmebaasi kasutamine (OPS.1.1.2, 1.1.3, 1.1.5, 1.1.6, 1.1.7, 2.1, 2.2, 3.1).

PostgreSQL andmebaaside majutuse ja haldusega on autori hinnangul otseselt seotud järgmised hankes mainitud moodulid:

- hoone ja ruumi turvalisus (INF): oluline andmekeskuste ja serveriruumide puhul, kus PostgreSQL andmebaase majutatakse, tagab füüsilise turvalisuse;
- võrguturvalisus (NET): andmebaasid peavad olema kaitstud võrgupõhiste rünnakute ja nõrkuste eest, eriti kui andmebaasid on kättesaadavad üle võrgu;
- serverite ja süsteemide turvalisus (SYS): need nõuded tagavad andmebaase hoidvate serverite ja operatsioonisüsteemide turvalisuse;
- rakenduste ja andmebaaside turvalisus (APP): käsitleb andmebaaside turvalisust;
- infoturve ja andmevahetus (CON): tagab, et andmeid hoitakse turvaliselt ja taastatakse efektiivselt hädaolukorras;
- õiguste haldus ja ligipääsud (ORP): tagab ainult volitatud isikute ligipääsu andmebaasidele;
- andmebaasi kasutamine ja haldus (OPS): otseselt seotud PostgreSQL andmebaaside haldusega, hõlmates IT-haldust, logimist ja süsteemihaldust.

Autori hinnangul ei pruugi PostreSQL andmebaaside majutuse ja halduse kontekstis esmatähtsad olla kõik mainitud moodulid, näiteks klientarvutite turvalisus. Kuigi see moodul on IT turvalisuse üldises raamistikus oluline, võib selle tähtsus konkreetse teenuse puhul olla piiratum, kui sellel ei ole otseselt mõju andmebaaside operatsioonidele või infrastruktuurile. Sellistes olukordades on oluline, et hankijad määratleksid selgelt, millised turvameetmed on kriitilised just teenuse põhifunktsionaalsuse ja -turvalisuse tagamiseks.

Andmebaasi majutusteenuse hanke dokumentatsioon sisaldab täiendavaid punkte, mis täpsustavad nõudeid andmekeskusele, andmekeskuste füüsilistele ligipääsudele, turvalisuse ja andmekaitsele, varundusele ja andmetaastele, klienditoele ja monitooringule [39].

5.2.2 Hanke analüüs

Käesolevas analüüsis uurib autor, kuidas hankija poolt hankes kirjeldatud teenuse E-ITSi moodulite sisu ja ülesanded jaotuvad hankija ja teenuseandja vahel. Meetmete vastutaja kirjeldused on autori hinnangud vastutaja määramisel. Hankes oli nõutud minimaalselt vastavust 2022. aasta E-ITSi[2] versioonile, antud versioonile toetutakse ka analüüsis. Detailne analüüs on toodud Lisas 1. Autor määratleb rollijaotuse, kus hankija vastutab turvapoliitikate väljatöötamise, kehtestamise ja järelevalve eest. See vastutus hõlmab turvanõuete sõnastamist, poliitikate ajakohasuse säilitamist ning turvameetmete üldist koordineerimist ja hindamist. Teisalt on teenuseandja kohustatud rakendama neid poliitikaid, mis hõlmavad turvaprotokollide implementeerimist ja haldamist vastavalt hankija ettekirjutustele.

Infrastruktuuri turvalisus (INF)

Teenuseandja vastutab turvameetmete eest, sealhulgas füüsilise turvalisuse tagamise ja juurdepääsukontrolli süsteemide ning tehnilise taristu haldamise eest. Teenuseandja peamine roll on tagada, et infrastruktuur vastab kehtestatud turvastandarditele, määratledes ja kontrollides turvanõuete täitmist.

Võrguturvalisus (NET)

[2] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/isms-noouded

Hankija vastutab võrgu turvapoliitika süstemaatilise väljatöötamise ja pideva ajakohastamise eest, hõlmates võrgu struktuuri, segmenteerimist ja demilitariseeritud tsoonide määratlemist ning võrgu turvanõuete regulaarset dokumenteerimist ja uuendamist, mis on kooskõlas organisatsiooni üldise infoturvapoliitikaga.

Hankija töötab välja võrgu käitusjuhendi, mis defineerib organisatsiooni sisemised võrguhaldusprotseduurid. Protsess sisaldab nõuete dokumenteerimist ja võrguhalduse juhendi koostamist, mis katab võrguteenused, haldusvahendid ja turvameetmed.

Hankija määrab tulemüüri valiku nõuded, integreerib tulemüüri avariivalmenduse organisatsiooni avariivalmenduse plaaniga, koostab tulemüüride turvajuhendi ja kehtestab tulemüüri- ning filtreerimisreeglid. Hankija viib läbi võrguhalduse regulaarsed ülevaatused, määrab logimiseks olulised sündmused.

Teenuseandja on kohustatud järgima hankija koostatud juhiseid võrgu turvalise toimimise tagamiseks ning võib pakkuda võrgusündmuste logimisteenuseid. Teenuseandja rakendab hankija määratletud ruuterite turvanõudeid ja osaleb avariivalmiduse plaanis, tagades operatiivsete ülesannete, nagu turvaparanduste rakendamine ja rikkeotsing, täitmise.

Teenuseandja tagab võrgu turvalisuse, jagades selle füüsiliselt eraldatud tsoonideks vastavalt turbenõuetele. Kliendid ja teenused hoitakse eraldi võrgusegmentides. Teenuseandja kasutab turvalisi sidekanaleid andmeedastuseks ja suunab kogu internetiliikluse läbi tulemüüri. Samuti on rakendatud kahetasemeline tulemüürisüsteemi ja IT-taristu kaitsmiseks kasutatakse VLAN-i, mis vastab kehtivatele turvanõuetele.

Teenuse andja peab regulaarselt andmevarundust korraldama, hoidma kellaaegu sünkroonis ning tagama võrguhalduseks vajaliku andmeside turvalisuse. Lisaks peab teenuseandja piirama SNMP protokolli kasutamist, dokumenteerima võrguhalduse tegevused ning tagama süsteemi turvalise konfigureerimise. Teenuseandja ülesandeks on korraldada ka oma töötajate võrguhalduse koolitusi, piirata halduspääsu ja haldusfunktsioone ning tagada keskne konfiguratsioonihaldus ning võrgukomponentide seire.

Haldustööjaamade turvaline paigutus ja virtuaalsete haldusvõrkude kasutamine on samuti teenuseandja vastutusalas. Tulemüüri turvalisuseks peab teenuseandja tagama ligipääsukontrolli haldusliidestele ja logima olulised sündmused, hoidma tulemüüri kella sünkroniseeris ja jälgima tulemüüri seiretulemusi tehes regulaarseid kontrolle ja teste.

Süsteemide turvalisus (SYS)

Hankija ülesanded keskenduvad turvanõuete määratlemisele ja juurdepääsude piiramisele, hõlmates turvajuhiste koostamist, turvaseadistuste rakendamist ja turvaliste autentimisprotseduuride väljatöötamist. Hankija ülesandeks on määratleda juurdepääsuõigused eelnevalt autoriseeritud isikutele, kahjurvaratõrje rakendamine, ja enne kasutuselevõttu süsteemi (serveri) sooritusvõime, mälumahtude ning läbilaskevõime hindamist. Hankija vastutab turvanõuete määratlemise eest Linuxi ja Unixi serveritele, tagades kasutajanimede, UID-de ja GID-de unikaalsuse süsteemses halduses.

Hankija vastutab virtualiseerimissüsteemi arhitektuuri ja kavandamise eest nii, et see vastaks organisatsiooni IT-poliitikatele. Hankija määratleb ja dokumenteerib konteinerduse strateegilise planeerimise, sealhulgas turvaliste konteineritõmmiste loomise, rakenduste ja teenuste sobivuse testimise, ning ressursipiirangute kehtestamise.

Ühiselt vastutavad hankija ja teenuseandja virtualiseerimiskeskkonna turvalise konfiguratsiooni ja konteinerdatud IT-süsteemide käitamise eest, määrates kasutajate autentimisnõuded ja tagades süsteemi regulaarsete läbivaatuste kaudu riistvara vastavuse virtualiseerimislahenduse nõuetele. Vastutuste hulka kuulub süsteemide toimivuse seire, turvauuenduste paigaldamine ja metaandmete kaitse volitamata muudatuste eest.

Teenuseandja on kohustatud kaitsma haldusliideseid, desaktiveerima tarbetud liidesed ja teenused ning dokumenteerima serveri konfiguratsiooni. Lisaks peab teenuseandja piirama kasutajatele ja rakendustele antavat salvestusruumi ning desaktiveerima mittevajalikud serverikomponentide püsivara funktsioonid. Teenuseandja tagab serverite piisava võimsuse ja aku kestvuse ning kaitseb neid lokaalse paketifiltriga. Teenuseandja koostab selge serveri käidudokumentatsiooni ja vastutab süsteemide seire eest, et tagada nende turvalisus ja toimimine. Krüpteerimine, tarkvarapakettide turvaline installimine ning volitamata õiguste laiendamise takistamine kuuluvad teenuseandja vastutusalasse. Virtualiseerimise ja konteinerite puhul on teenuseandja vastutav nende turvalise rakendamise, haldamise ja konfiguratsiooni eest, rakendades turvamehhanisme ja tagades konfiguratsiooniandmete turvalisuse ning pideva seire.

Rakenduste ja andmebaaside turvalisus (APP)
Hankija töötab välja turvapoliitikad rakendustele ja andmebaasidele, määratleb turvameetmed ning tagab, et need on dokumenteeritud ja ajakohased. Hankija koostab andmebaasi turvalisuse tõstmiseks vajalikud turvajuhendid ja kontroll-loendid, mida teenuseandja rakendab. Hankija koostab tüüpkonfiguratsiooni, teenuseandja järgib seda, kontrolli teostab hankija. Andmebaasisüsteemi seire eest vastutab teenuseandja, hankija kontrollib, et seire vastab tema spetsiifilistele vajadustele.

Teenuseandja tagab andmebaasisüsteemi turvalisuse, tagades regulaarse varundamise, sealhulgas ka enne andmebaasi loomist, ning taastamisparameetrite määramise vastavalt andmete kaitsetarbele. Vajadusel kohandab teenuseandja varunduse kontseptsiooni. Samuti seab teenuseandja piirangud andmebaasi linkidele, andes juurdepääsuõigused ainult määratud isikutele. Lisaks krüpteerib teenuseandja andmebaasiühendused, et tagada nende vastavus kaitsetarbele ning rakendab sobivaid krüpteerimisprotseduure ja -mehhanisme.

Kontseptsioonid ja metoodikad (CON)
Isikuandmete kaitse eest vastutab suures osas hankija organisatsiooni juhtkond, sinna on kaasatud järgmised meetmed: isikuandmete kaitse kavandamine, andmekaitsespetsialisti määramine, andmekaitsepoliitika väljatöötamine, isikuandmete töötluse kaardistamine ja turvameetmete dokumenteerimine. Samuti on vajalik hankijal töötajate teadlikkust tõsta ja piirata juurdepääsu isikuandmetele.

Hankija koostab andmevarunduse strateegia koos varundatavate andmete registriga, määratleb varunduse mõjurid, koostab varunduse eeskirjad, valib sobiva varundussüsteemi, sõlmib teenusetaseme lepingud ja testib regulaarselt varundussüsteemi toimimist.

Isikuandmete kaitse ja andmevarunduse kontseptsioon hõlmavad koostööd hankija ja teenuseandja vahel, et tagada turvameetmete järgimine, isikuandmete krüpteerimine ja andmetöötlustoimingute logimine. Hankija seab turvanõuded ja -poliitikad, mida teenuseandja rakendab, sealhulgas varunduse regulaarsus, korraldus ning turvastandardid.

Olles hankija andmete füüsiline hoidja, peab teenuseandja looma piiratud pääsuga alad, kehtestama juurdepääsureeglid ning rakendama tehnilisi juurdepääsu- ja valvesüsteeme isikuandmete füüsilise turvalisuse tagamiseks. Teenuseandja peab välja töötama külaliste haldamise protseduurid, et tagada isikuandmete töötlemise aladele kontrollitud ja turvaline juurdepääs. Teenuseandja tagab, et isikuandmete saatmiseks avaliku võrgu kaudu kasutatakse turvalisi ja krüpteeritud protokolle. Samuti on teenuseandja vastutav varunduseks kasutatavate andmekandjate turvalise säilituse eest, hoides neid lähtesüsteemist eraldi ja järgides andmete säilitamise poliitikat.

Organisatsioon ja personal (ORP)
Hankija on peamine vastutaja kasutajakontode halduseeskirjade arendamise ja kinnitamise eest, tagades, et need on kooskõlas organisatsiooni sisepoliitikaga. Need eeskirjad kujutavad endast laia spektrit kohustusi, alates IT kasutamise nõuetest kuni füüsilise ligipääsu haldamiseni. Hankija roll hõlmab turvaliste autentimis- ja juurdepääsuõiguste protseduuride väljatöötamist ning identiteedi- ja õiguste halduse süsteemide valikut, mis toetavad organisatsiooni äriprotsesse ja turvanõudeid.

Teenuseandja kohustus on rakendada ja hallata hankija loodud poliitikaid, sealhulgas on pääsuõiguste, paroolipoliitika ja autentimisnõuete aktiivne jõustamine.

Teenuseandja peab rakendama mitmikautentimist eeliskontode kaitsmiseks, mis aitab süsteemi kaitsta väliste ründajate eest ja hoida ära õiguste volitamata laiendamise. Lisaks on teenuseandja kohustus tagada, et kasutajakontode kasutamine oleks tõhusalt reguleeritud tagades, et kasutajad logivad regulaarselt oma kontosid kasutades süsteemist välja pärast ülesannete täitmist. Juurdepääsu IT-süsteemidele reguleeritakse vastavalt kehtestatud pääsupoliitikatele kasutades töötaja ülesannetega vastavuses olevaid standardseid õiguste profiile. Teenuseandja peab tagama, et paroole ei talletata avateksti kujul ning need edastatakse alati krüpteeritult. Paroolide vahetamine toimub alati konkreetse põhjusega. Vaikimisi paroolid ja sisselogimissätted muudetakse esimesel võimalusel piisavalt tugevateks.

Käidutööd (OPS)
Hankija vastutab IT-haldurite kontode haldamise eest, hõlmates nende blokeerimist ja juurdepääsuõiguste tühistamist töölt lahkumisel ning uute kontaktisikute määramist kolmandate osapooltega suhtlemisel. Hankija sätestab IT-süsteemide haldamise rollid ja kasutajaõiguste alused, tagades, et neid põhimõtteid rakendatakse nõuetekohaselt. Hankija on vastutav IT-haldurite asendamise protseduuri, halduskontode autentimismeetodite ning allhangete turvanõuete kehtestamise eest. Hankija koostab ja kontrollib korrapäraselt teenuselepinguid, et veenduda turvameetmete asjakohasuses ja vastavuses organisatsiooni nõuetele ning tagab lepingute kooskõla organisatsiooni avariivalmenduse plaanidega.

Teenuseandja vastutab hankija juurdepääsuõiguste nõuetekohase rakendamise, logimisnõuete täitmise ja logide terviklikkuse tagamise eest. Teenuseandja ülesanded hõlmavad hankija tehniliste muudatuste läbiviimist, hankija antud turvaliste seadistuste loomist, tarkvara testimisprotsesse ja ühiselt koos hankijaga funktsionaalsete ning regressioonitestide korraldamist tarkvara uuendamisel. Teenuseandja rakendab ja haldab hankija määratletud pilvteenuste turvanõudeid ning süsteemihalduse seiret, logimist ja teavitab oluliste sündmuste puhul, järgides hankija kehtestatud turvanõudeid ja -eeskirju.

Teenuseandja vastutab IT-haldurite ja nende asendajate personaalsete eeliskontode kasutuselevõtu eest, rakenduste halduse, haldustoimingute dokumenteerimise ja kasutajatega

kooskõlastamise eest. Samuti on teenuseandja ülesandeks tagada halduspääsu tehniline eraldamine, IT-halduse toimingute ajastamine ja IT-komponentide konfiguratsiooni varundamine. Teenuseandja vastutab uue riistvara testimise ja kasutuselevõtu, sündmuste logimise seadistamise ning logiandmete arhiveerimise eest, tagades kõigi nõuetekohase täitmise vastavalt kehtivatele õigusaktidele ja turvastandarditele.

Lisaks vastutab teenuseandja tarkvara funktsionaaltestimise, testandmete pseudonüümimise ning testijate valiku eest, et tagada testide usaldusväärsus ja tundlike andmete kaitse. Süsteemihaldusega seotud ülesannete eest vastutab teenuseandja, tagades süsteemide tervikluse, konfigureerimise korrektsuse ja andmete turvalisuse. Teenuseandja vastutab simultaanteeninduse võimekuse hindamise ja personali kasutamise korra eest, tagades klientide andmete turvalise käsitlemise ja teenuseandja vastavuse kehtivatele nõuetele.

Kokkuvõttes on soovitud meetmete rakendajaks suures osas hankija ise, seda turvapoliitika kujundamisel ja järelevalvel, tagades, et turvameetmed ja protseduurid on kooskõlas organisatsiooni üldiste eesmärkidega. Hankija peamised ülesanded on turvanõuete määratlemine, poliitikate kehtestamine ja järelevalvemeetmete rakendamine. Hankija vastutusalad laienevad võrgu, süsteemide, rakenduste ja andmebaaside turvalisuse tagamisele, samuti turvapoliitika ja personalihalduse protseduuride väljatöötamisele ja rakendamisele organisatsioonis. Need ülesanded nõuavad sügavat arusaamist organisatsiooni sisemistest protsessidest ning ei ole võimalik allhankena pakkuda.

Teenuseandja peamine ülesanne on hankija seatud turvapoliitikate ja protseduuride igapäevane rakendamine ja haldamine. Teenuseandja aitab organisatsiooni operatiivset turvalisust säilitada ja omab kohustust hankija seatud poliitikate nõuetekohaseks rakendamiseks. Hankija ja teenuseandja koostöö ulatub kriisijuhtimise ja avariiolukordade planeerimiseni.

Teenuseandja vastutab oma infrastruktuuri turvalisuse eest, tagades füüsilise turvalisuse ja juurdepääsukontrolli, võrgu eraldamise ning turvalise andmeside. Võrdset tähtsust oma ka regulaarne andmevarundus, kellaaegade sünkroonimine ja võrguhalduse turvalisus. Lisaks peab teenuseandja haldama IT-süsteeme ja konfiguratsioone, koolitama töötajaid, jälgima tulemüüride toimivust ja logima olulisi sündmusi. Tähtis on ka süsteemide seire, krüpteerimine ja turvalise tarkvara kasutuselevõtt, tagades kogu IT-taristu ja sellega seotud tegevuste nõuetekohase haldamise ning turvalisuse. Teenuseandja roll hõlmab ka kasutajakontode reguleerimist, paroolihaldust ja turvalist haldusliideste kaitset.

5.3 Riigihange „Infosüsteemide majutusteenuse tellimine ETIS ja EHIS"

Infosüsteemide majutusteenuse tellimine ETIS ja EHIS hankedokument kirjeldab tellitavat teenust, mis käsitleb EHISe ja ETISe keskkondade majutust ja administreerimisteenust [40]. Hange on valitud autori poolt vaatlusaluseks, kuna sisaldab tehnilises kirjelduses ISKE viiteid, ISKE ja E-ITSi vastavustabel kehtib vaid E-ITSi 2020. aasta versiooni kohta ning pole üks-ühele üle kantav. Näide illustreerib hankeid, milles soovitakse vastavust ISKE-le.

5.3.1 Hanke ülevaade

Hetkeolukord on kirjeldatud vajadusena hankija süsteemid füüsiliselt kolida teenuseandja majutuskeskkonda. Hankija infosüsteemide majutamiseks vajalik taristu ja selle haldamine sisaldab järgmisi alaosasid: serverite ja teiste süsteemide majutamiseks vajalik taristu, infosüsteemide majutusteenus serveriruumis, internetiühendus, tulemüüriteenus, serverite ja muu taristu riistvara ning tarkvara (nii süsteemse kui ka rakendustarkvara) haldamisteenus [40].

Infosüsteemide majutusteenuse tellimine ETIS ja EHIS hankedokumendis on iga teenuse osa käsitlemas konkreetseid ülesandeid ja nõudeid, mis tagavad infosüsteemide tõhusa ja turvalise majutamise ning haldamise [40]. Teenuse osutamisel tuleb teenuseandjal arvestada ISKE M turbetaseme nõuetega, tagades infosüsteemide ja nendega seotud andmete ja tarkvara turvalisuse.

Majutusteenuse tellimise hankedokumendis on serveriruumide nõuetes eraldi välja toodud nõue teenuseandja pakutava majutusteenuse ISKE-le samaväärse infoturbestandardi rakendamise ja auditeerimise kohta, näiteks ISO või E-ITS [40]. EHISele on määratud ISKE „keskmine“ turvalisuse tase (K2T2S2). See tähendab, et EHISe toodangu keskkond peab olema kättesaadav 99,9% ajast.

ISKE süsteem jagab turbeastmed kolmeks: madal (L), keskmine (M) ja kõrge (H). Infovarade turbeastme määramise järgselt tuleb leida igale infovarale vastavad tüüpmoodulid. Tüüpmoodulid sisaldavad turbemeetmete kirjeldusi, mis peavad olema rakendatud, et tagada nõutav turvalisuse tase. Astme M saavutamiseks on vajalik rakendada ka turbemeetmeid, mis on astmega L.

Kuna ISKE oli hanke väljastamise ajaks kehtivuse kaotanud, pidas autor hankija soovitud teenuse EHISe ja ETISe keskkondade majutus ja administreerimine [40] tehnilist kirjeldust aluseks võttes asjakohaseks järgmisi E-ITSi mooduleid:

- INF.1, INF.2, INF.3, INF.5, INF.12, INF.13: tagab füüsilise turvalisuse;
- ORP.4 Identiteedi- ja õiguste haldus: tagamaks, et õigused ja identiteedid on õigesti hallatud;
- OPS.1.1.2 IT-süsteemide haldus: teenus hõlmab serverite haldust;
- OPS.1.1.3 Paiga- ja muudatusehaldus: infosüsteemide nõuetekohane töö tagamiseks;
- OPS.1.1.4 Kaitse kahjurprogrammide eest: süsteemide kaitse kahjurprogrammide ja pahavara eest;
- OPS.1.1.5 Logimine: tegevuste logimine;
- OPS.1.1.6 Tarkvara testimine ja kasutuselevõtt: tagamaks uute rakenduste ja süsteemide turvaline kasutuselevõtt;
- DER.2.1 Turvaintsidentide käsitlus: võimalike turvaintsidentide efektiivne käsitlus;
- NET.3.2 Tulemüür: eraldab infosüsteemide sisevõrku välisest võrkudest;
- CON.3 Andmevarunduse kontseptsioon: tagamaks andmete säilivus ja taastatavus.

5.3.2 Hanke analüüs

Käesolevas analüüsis uurib autor, kuidas ülaltoodud E-ITSi meetmete ülesanded jaotuvad hankija ja teenuseandja vahel. Meetmete vastutaja kirjeldused on autori hinnangud vastutaja määramisel. Analüüs baseerub 2022. aasta E-ITSi versioonil[3]. E-ITSi juhendite veebilehel olev võrdlustabel ISKE ja E-ITSi meetmete vahel kirjeldab E-ITS etalonturbe mooduli meetmete 2020. versiooni ja ISKE 8.06 meetmete turbeaste L ja M omavahelist seost [6]. Võrdlus on esitatud pigem informatiivse ülevaatena, mis aitab mõista turvameetmete rakendamise keerukust, millega teenuseandjad pakkumiste koostamisel silmitsi seisavad. Põhjalik analüüs on toodud välja Lisas 2, milles autor määratleb meetmepõhiselt rollijaotuse.

Infrastruktuuri turvalisus (INF)

[3] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/isms-noouded Hanke väljastamise ajal oli kehtiv E-ITSi versioon 2022

E-ITSi turvameetmete rakendamise eest vastutab teenuseandja sellistes valdkondades nagu hoone üldine turvalisus, serveriruumid ja andmekeskused, tehnilise taristu ruumid, kaabeldus ning hoonete tehniline haldus. INF.12: Kaabeldus ja INF.13: Hoonete tehniline haldus, mille eest samuti vastutab teenuseandja, puuduvad ISKEst.

Organisatsioon ja personal (ORP)
Hankija vastutab organisatsiooni sisepoliitikaga kooskõlas olevate kasutajakontode halduseeskirjade koostamise ja kinnitamise eest. See hõlmab juurdepääsuõiguste määramist, IT kasutamise nõuete kehtestamist, füüsilise ligipääsu kontrolli ning turvaliste parooliprotseduuride loomist. Hankija valib autentimisteenused ja suunab töötajaid nende kasutamisel, tagades, et kasutatavad identiteedi- ja õiguste halduse süsteemid toetavad organisatsiooni äriprotsesse ja turvanõudeid.

Teenuseandja ülesanded keskenduvad hankija määratud protseduuride ja poliitikate rakendamisele ja haldamisele, mis hõlmavad pääsuõiguste juhtimist, paroolikorra rakendamist ja autentimisnõuete jõustamist. Teenuseandja tagab IT-süsteemide ja rakenduste turvalise autentimise, rakendades hankija poolt koostatud identiteedi- ja õiguste halduse protseduure.

Teenuseandja vastutab eeliskontode kaitsmise eest kasutades mitmikautentimist, et kaitsta neid väliste ründajate ja õiguste volitamatu laiendamise eest. Teenuseandja on vastutav kasutajakontode kasutamise kontrollimise eest, tagades, et kasutajad logiksid pärast ülesannete täitmist alati süsteemist välja. Teenuseandja vastutab IT-süsteemidele juurdepääsu reguleerimise eest, järgides kehtestatud pääsupoliitikaid ja kasutades standardseid õiguste profiile, mis vastavad töötaja ülesannetele. Teenuseandja on kohustatud tagama paroolide turvalisuse IT-süsteemides, hoides paroole krüpteeritult ning tagades, et paroolid vahetatakse piisavalt tugevate vastu.

ISKE sisaldab kõiki E-ITSi organisatsiooni ja personali sisaldavaid meetmeid.

Käidutööd (OPS)
Hankija vastutab IT-halduri rolli, kasutajaõiguste ja haldusrollide määramise eest, et tagada organisatsiooni vajadustele vastavus ning õiguste minimaalsuse põhimõte. Hankija kontrollib IT-haldusega seotud poliitikate ja protseduuride korrektset rakendamist, sealhulgas kontode blokeerimist ja pääsuõiguste eemaldamist peale IT-halduri lahkumist. Hankija määrab autentimismehhanismid ja IT-haldurite asendamise korra, autentimismehhanismide rakendamist ja järgimist kontrollib teenuseandja. Hankija vastutab logimisnõuete kehtestamise eest, teenuseandja tagab logimise nõuetekohase toimimise ja logide terviklikkuse.

Hankija kehtestab paiga- ja muudatusehalduse korra, hangib usaldusväärsetest allikatest tarkvara ning dokumenteerib IT-süsteemide muudatused. Hankija kehtestab poliitikad, mis tagavad muudatusehalduse kooskõla organisatsiooni äriprotsessidega, teenuseandja teostab muudatuste tehnilist läbiviimist ja tagab turvalise seadistuse.

Hankija koostab tõrjekontseptsiooni, dokumenteerib turvamehhanismid ja korraldab kasutajakoolitusi. Teenuseandja on selles protsessis konsultandina, pakkudes ekspertiisi ja nõuandeid kahjurvaratõrje tarkvara valikul.

Hankija on vastutav tarkvara testimise ja kasutuselevõtu protsessi kavandamise ning vastuvõtukorra kehtestamise eest. Hankija ja teenuseandja jagavad vastutust tarkvara

testimisprotsesside läbiviimise eest, sealhulgas mittefunktsionaalsete ja regressioontestide nõuete määramise ja nende teostamise eest.

Teenuseandja peab haldama personaalsete eeliskontode loomist ja nende järelevalvet, eeliskontod on mõeldud üksnes haldustoiminguteks ning nende tegevuste jälgimine suurendab kasutamise läbipaistvust. Teenuseandja kohustatud määratlema rakenduste halduse ülesannete jaotuse ja dokumenteerimise. Juurdepääsu tehniline eraldamine on samuti teenuseandja vastutusvaldkonnas, kasutades eraldatud võrgusegmente ja hüppeservereid, mis piiravad haldusliideste juurdepääsu ning takistavad otsesid ühendusi välisvõrguga.

Lisaks peab teenuseandja tagama uue tarkvara põhjaliku testimise enne selle kasutuselevõttu, et veenduda selle nõuetekohases toimimises ja süsteemiga ühilduvuses. Tarkvara funktsionaalsust ja vastavust kontrollitakse põhjalikult, tagades, et kõik funktsioonid töötavad ootuspäraselt. Testandmete anonüümimine on oluline, et kaitsta tundlikke andmeid testkeskkonnas ja tagada testide usaldusväärsus. Testkeskkonna lahutamine käidukeskkonnast ning selle ettevalmistamine vastavalt juhistele on vajalik, et vältida võimalikke riske ja häireid käidukeskkonnas.

Teenuseandja vastutus on korraldada sündmuste logimine, sünkroniseerida kellasid ja arhiveerida logiandmeid järgides kehtivaid eeskirju ja õigusaktide.

ISKE ei kata järgnevaid E-ITSi meetmeid: kõik OPS.1.1.2, OPS.1.1.6.M2–OPS.1.1.6.M13. ISKEs on kirjeldatud kõik E-ITSi OPS 1.1.3, OPS 1.1.4, OPS 1.1.5 meetmed. ISKE meetmed L ja M on E-ITSis kõrgmeetmete hulgas (OPS.1.1.4.M10, OPS.1.1.4.M11, OPS.1.1.4.M12, OPS.1.1.4.M12, OPS.1.1.4.M13, OPS.1.1.4.M14, OPS.1.1.4.M15, OPS.1.1.5.M11, OPS.1.1.5.M12, OPS.1.1.5.M12, OPS.1.1.5.M13, OPS.1.1.6.M14).

Avastamine ja reageerimine (DER)
Hankija määratleb sündmused, mis kvalifitseeruvad turvaintsidentideks, ning koostab ja ajakohastab regulaarselt turvaintsidentide käsitluse protsessijuhendit. Hankija loob süsteemi, kuidas teavitatakse asjaosalisi turvaintsidentidest ja dokumenteerib erinevat tüüpi intsidentide käsitlemise metoodikad. Hankija töötab välja turvaintsidentide toime piiramiseks tegevuskavad ja hindamisprotseduurid ning integreerib need protsessid turbe- ja avariihaldusega.

Koostöös teenuseandjaga on määratud vastutused ja kontaktisikud turvaintsidentide ühiseks käsitluseks, tagades asjaosalistele vajaliku koolituse ja ajakohase kontaktinformatsiooni. Koostöös on loodud protseduurid töökeskkonna taastamiseks pärast turvaintsidenti ja moodustatud muutuva koosseisuga turvaintsidentide käsitluse töörühm, mis kohandub vastavalt intsidentide tüübile. Hankija on varustanud IT-talituse töötajaid vajalike vahendite ja kontroll-küsimustikega turvaintsidentide tuvastamiseks, teenuseandja töötajad on läbinud asjakohase koolituse ja tutvunud turvaintsidentide käsitluse juhendiga.

Teenuseandja vastutab turvaintsidendi lahendamise kordade eest, omades vajalikku teadmist, ressursse ja juurdepääsu süsteemidele, mis võimaldavad teenuseandjal turvaintsidentidele kiiresti ja tõhusalt reageerida. Lisaks on teenuseandjal spetsialiseeritud personaal ja tehnoloogilised vahendid, mis võimaldavad teenuseandjal võtta käsile kiireid ja tõhusaid meetmeid, et lahendada intsidente ning tagada teenuste ja andmete turvalisus.

ISKEs on kõik E-ITSi mooduli DER2.1 meetmed kirjeldatud. ISKE meetmed L ja M on E-ITSis kõrgmeetmete hulgas (DER.2.1.M19, DER.2.1.M19, DER.2.1.M20, DER.2.1.M20, DER.2.1.M21, DER.2.1.M21, DER.2.1.M22, DER.2.1.M22).

Võrguturvalisus (NET)
Hankija vastutab tulemüüri spetsiifiliste nõuete määratlemise eest hankimisel, tagades, et need vastavad organisatsiooni infoturbepoliitikale. Hankija vastutab tulemüüri avariijuurdepääsu protsesside olemasolu ja füüsilise juurdepääsu tagamise eest avariijuhtumite korral. Tulemüüri avariivalmendus on integreeritud osana organisatsiooni üldisesse avariivalmiduse plaani.

Ühiste kohustuste raames koostab hankija tulemüüride turvajuhendi, mis põhineb organisatsiooni turvapoliitikal, teenuseandja tagab, et juhendit järgitakse korrektselt. Hankija kehtestab tulemüüri- ja filtreerimisreeglid, teenuseandja rakendab ja haldab neid. Teenuseandja vastutab tulemüüri turvalise konfigureerimise eest, samal ajal kui hankija kontrollib, et konfiguratsioon vastab organisatsiooni turvanõuetele. Teenuseandja dokumenteerib turvalisust mõjutavad toimingud, mille hankija lisab oma käidudokumentatsiooni.

Teenuseandja vastutab, et tulemüüri haldusliidestele oleks ligipääs ainult määratud IP-aadressidelt või -vahemikust ning et ebausaldusväärsetest võrkudest ei oleks juurdepääsu haldusliidestele. Teenuseandja peab logima olulised turvasündmused, nagu haldusliidesesse sisselogimised ja konfiguratsioonimuudatused, ning tagama, et tulemüüri tehtud toimingud on logitud automaatselt. Teenuseandja vastutab IPv4 ja IPv6 killuründe tõrjumise eest paketifiltris ning turvalise P-A-P-struktuuri rajamise eest. Teenuseandja ülesandeks on tagada, et tulemüüri kellaaeg on sünkroniseeritud. Teenuseandja vastutab tulemüüri haldusliideste turvalisuse, UDP-tulva ja TCP SYN-tulva tõrje, ning järjenumbri äraarvamise eest paketifiltris. Teenuseandja korraldab tulemüüri haldamise ainult eraldi haldusvõrgu kaudu ning vastutab tulemüüri seire ja seiretulemuste analüüsi eest. Teenuseandja kohustus on regulaarselt läbi vaadata ja testida tulemüüri teadaolevate turvaprobleemide suhtes ning dokumenteerida läbivaatuste tulemused, et tagada tulemüüri turvalisus ja vastavus turvanõuetele.

ISKEs on kõik E-ITS NET.3.2 meetmed kirjeldatud. ISKE meetmed L ja M on E-ITSis kõrgmeetmete hulgas (NET.3.2.M20, NET.3.2.M20, NET.3.2.M21, NET.3.2.M22, NET.3.2.M28, NET.3.2.M28, NET.3.2.M29).

Kontseptsioonid ja metoodikad (CON)
Hankija koostab varundatavate andmete registri ja andmevarunduseeskirja, määratleb andmevarunduse mõjurid ning töötab välja andmevarunduse kontseptsiooni ja kooskõlastab selle vastutajatega. Hankija valib sobiva andmevarundussüsteemi, soetab selle ja sõlmib teenusetasemelepingud ning määrab süsteemi efektiivse toimimise tingimused. Hankija testib regulaarselt andmevarunduse toimimist ja varundatud andmete taastamist.

Hankija määrab andmevarunduse regulaarsuse ja korralduse, varukoopiate turvastandardid ja -nõuded ning teavitab nendest organisatsiooni töötajaid. Teenuseandja vastutab hankija kehtestatud ajakava, protseduuride ning turvastandardite ja -nõuete järgimise eest.

Teenuseandja vastutab varunduseks kasutatavate andmekandjate turvalise säilituse eest, hoides andmekandjaid lähtesüsteemist eraldi. Teenuseandja peab tagama andmete turvalise säilituse vähemalt nõutud andmesäilitustähtaegade ulatuses.

ISKEs on kõik E-ITS CON.3 meetmed kirjeldatud. ISKE meetmed L ja M on E-ITSis kõrgmeetmete hulgas (CON.3.M13, CON.3.M13, CON.3.M13).

Kokkuvõtvalt vastutab teenuseandja hoone üldise turvalisuse, serveriruumide, andmekeskuste ning tehnilise taristu eest. Organisatsiooni ja personali valdkonnas töötab hankija välja kasutajakontode halduseeskirjad, määrab juurdepääsuõigused ja valib autentimisteenuseid, mille teenuseandja praktikas rakendab. Käidutööde puhul haldab hankija IT-halduri rolle ja logimisnõudeid, määrab muudatuste halduse korra ning mida teenuseandja järgib tagades nende nõuetekohase täitmise. Turvaintsidentide avastamise ja reageerimise osas koostab hankija juhendid ja tegevuskavad ning teenuseandja osaleb intsidentide lahendamisel. Võrguturvalisuse kontekstis määratleb hankija tulemüüri nõuded ja kehtestab turvapoliitikad, mida teenuseandja rakendab ja jälgib. Andmevarunduse puhul loob hankija andmevarunduse kontseptsioonid ja protseduurid, mida teenuseandja järgib.

Lisaks näitab analüüs, et ISKE meetmeid ei ole võimalik üks-ühele teisendada E-ITSi meetmeteks, tulenevalt nende turbeastmete erinevustest.

6. Kontrollnimekiri hanke tehnilise kirjelduse koostamiseks

Küberturvalisuse seaduses [4] on sätestatud olukord, kus teenuse osutaja kasutab välise teenuseandja teenuseid või delegeerib süsteemi haldamise teisele isikule. Antud sätte kohaselt on teenuse osutaja kohustatud tagama, et süsteemi haldav teine isik rakendab vajalikke turvameetmeid. See tähendab, et teenuse osutaja kannab vastutust süsteemi turvalisuse eest, olenemata sellest, kas haldamine toimub teenuse osutaja enda või teise isiku poolt. Antud punkti silmas pidades ja hankija teadlikkuse tõstmiseks oma kasutuses oleva IT-vara turvameetmete rakendamisel on autor koostanud kontrollnimekirjade komplekti, aitamaks määratleda ja teadvustada vastutajat ning sellega tõsta ka üldist organisatsiooni IT-turvalisuse taset.

Autor koostas kontrollnimekirja üldise dokumentatsiooni ja tegevuste kohta, hangitava teenuse kontrollnimekirjad teenustele Kubernetes ja veebiserver ning juhendi valitud meetmete viimiseks hanke tehnilisse kirjeldusse. Kontrollnimekirjad on struktureeritud tegevuste loendid, mis kirjeldavad tegevusi, mis on vajalikud hankijal teostada hankes nõutavate küberturbe meetmete võimalikult täpseks kirjeldamiseks. Samuti on kontrollnimekirjad mõeldud teadvustama tehnilise meetme eest vastutaja rolli. Autor võttis kontrollnimekirjade koostamisel aluseks E-ITSi rakendusjuhise, viies selle ühtselt kokku riigihanke protsessiga, lisades juurde ISO/IEC 27002 kontrollidele vastavuse.

Kontrollnimekirja on lisatud soovitused IT-teenuste lahenduse arhitektilt, kelle igapäeva töö sisaldab hangete läbitöötamist. Näidistena on toodud teenuste Kubernetes ja veebiserver meetmete vastutaja jaotus. Kontrollnimekirjad on loodud eesmärgiga abistada hankijaid eduka hanke koostamisel ning vajadusepõhiste nõuete loetlemisel teenuseandjatele, mis on kooskõlas organisatsiooni riskihalduse ja infoturbe nõuetega. Kontrollnimekirjade loomisel on eeldatud, et rakendaja ei pruugi olla koostanud oma infoturbe dokumentatsiooni ning ei ole tutvunud E-ITSi rakendusjuhendiga. Praktilisel rakendamisel peab organisatsioon lähtuma konkreetsest tellitavast teenusest ning oma teenuse käideldavuse soovidest.

Kontrollnimekirja komplekti struktuur:

- üldine dokumentatsioon ja tegevused enne meetmete vastutaja määramist E-ITSi rakendusjuhendist lähtudes;
- hangitava teenuse kontrollnimekirjade näited: Kubernetese kontrollnimekiri ja veebiserveri kontrollnimekiri, mis sisaldavad rakenduvate meetmete analüüsi lähtudes vastutaja vaatepunktist kommentaaridega;
- juhend valitud meetmete viimiseks tehnilisse kirjeldusse ja edasised tegevused E-ITSi rakendusjuhendist lähtudes.

6.1 Üldine dokumentatsioon ja tegevused enne meetmete analüüsi E-ITSi rakendusjuhendist lähtudes

Selles jaotises olev tegevuste loetelu aitab kontrollida, kas E-ITSi jaoks vajalik dokumentatsioon on koostatud, ja meetmete määramiseks vajalikud sammud on tehtud. Sammud kujutavad endast infoturbe strateegia rakendamist, kitsendades skoopi ja tekitades esimese arusaamise sellest, millised on vajalikud meetmed, mis kohalduvad organisatsiooni poliitikaga. Ühtlasi viib hankija läbi ka riskianalüüsi, et tagada tellitava teenuse vastavus turvanõuete osas ning juhtimaks tarnijasuhetega seotud riske.

Tegevused on jaotatud 15 punktiks:

- Hanke vajaduse määratlemine – hankija määratleb, millist teenust hangitakse ja mida teenuseandja peab pakkuma, vajadusel viiakse läbi väärtusahela ja turu-uuringud ning konsulteeritakse turuosalistega, enne lõplikku otsustamist hangitava teenuse üle. Alustatakse hankelepingu tehniline kirjelduse koostamist. Nõue tuleneb riigihanke protsessist.

- Organisatsioonis on määratud infoturbe eest vastutaja, kes pole IT-juht, et lahutada vastuolulised ülesanded ja vastutusalad. Antud punkt vastab ISO/IEC 27002 kontrollile 5.2 „Infoturbe rollid ja vastutusalad" – infoturbe rollid ja vastutusalad tuleks määratleda ja jaotada vastavalt organisatsiooni vajadustele, ja ISO/IEC 27002 kontrollile 5.3 „Ülesannete jaotus" – vastuolulised ülesanded ja vastutusalad tuleks lahutada.

- Organisatsioonis on kehtestatud majanduslikke, tehnilisi, korralduslikke ja õiguslikke raamtingimusi ning infoturbe aspekte käsitlev väljasttellimise strateegia. Väljasttellimise strateegias on kirjeldatud väljasttellimise eesmärgid, võimalused ja riskid. Väljasttellitava teenuse organisatsioonil on vajalikud võimed, pädevus ja ressursid teenuse infoturbenõuete määramiseks ja kontrollimiseks. Antud punkt vastab E-ITSi meetmele – OPS.2.3: Väljasttellimine.

- Hankija on loonud oma organisatsioonikohase infoturbe poliitika, mis sisaldab infoturvaeesmärke, punkt vastab E-ITSi rakendusjuhendi infoturbe põhimõtetega, mis määratlevad suunised organisatsiooni infovarade turvalisuse tagamisel, ehk infoturbe korralduse. Punkt vastab ka ISO/IEC 27002 kontrollile 5.1 „Infoturbe poliitikad" – infoturbe poliitika ja teemakohased poliitikad tuleb määratleda, juhtkonna poolt heaks kiita, avaldada, teatada asjakohasele personalile ja asjakohastele huvipooltele, ning neid tuleb regulaarselt planeeritud intervallidega ja oluliste muudatuste korral üle vaadata.

- Rakenduste arendamisel või soetamisel tuleks kindlaks teha, määratleda ja heaks kiita infoturbe nõuded. Punkt vastab ISO/IEC 27002 kontrollile 8.26 „Rakenduste turvanõuded" – infoturbe nõuded tuleks tuvastada, määratleda ja heaks kiita rakenduste arendamisel või soetamisel.

- Hankija võtab varad arvele alustades äriprotsessist, seejärel äriprotsessi aluseks olev teave ja kaitseala sihtobjektid, punkt tuleneb E-ITSi rakendusjuhendist. Üheks levinud praktikaks on määrata iga vara jaoks omanik, kes seejärel vastutab selle igapäevase kaitse eest. Punkt vastab ISO/IEC 27002 kontrollile 5.9 „Informatsiooni ja muude seotud varade inventuur" – tuleks koostada ja hooldada informatsiooni ning muude seotud varade, sealhulgas nende omanike, inventuuri.

- Hankija määrab hangitava teenuse infoturbe kaitseala ja sihtobjektid (kogumi sihtobjekte, mida turbeprotsess hakkab edaspidi kaitsma), nõue toodud E-ITSi rakendusjuhendis.

- Hankija määrab hangitava äriprotsessi, kuhu hangitav teenus kuulub, kaitsetarbe – hinnang äriprotsessi kaitsetarbele tuleneb äriprotsessi poolt töödeldava teabe kaitsetarbest. Kaitsetarbe hinnang on kvalitatiivne, see antakse kolmeastmelisel skaalal – normaalne, suur, väga suur (vt Joonis 1 Kaitsetarbe maatriks). Kaitsetarbe määramiseks võib võtta aluseks E-ITS rakendusjuhendil põhinevad

kahjustsenaariumid, mida analüüsida nendega seotud ohtude võimalikkuse ja riskide realiseerumise tagajärgede kaalukuse vaatest. Punkt on pärit E-ITSi rakendusjuhendist ning vastab ka ISO/IEC 27002 kontrollile 5.12 „Informatsiooni klassifitseerimine" – informatsiooni tuleks klassifitseerida organisatsiooni infoturbe vajaduste põhjal, lähtudes konfidentsiaalsusest, terviklikkusest, kättesaadavusest ja asjakohaste huvipoolte nõuetest.

		Kaitsetarbe tase			
		N	**S**	**VS**	**Kokku**
Infoturbe komponent	**C**	1	2	3	C1
	I	1	2	3	I3
	A	1	2	3	A2
	Kaitsetarve				**C1-I3-A2**

Joonis 1 Kaitsetarbe maatriks [2]

- Hankija määratleb turbeviisi – tuletatakse äriprotsessile määratud kaitsetarbest, lähtutakse organisatsioonile rakendatavatest regulatsioonidest ning otsustatakse organisatsiooni infoturbe küpsuse pealt. Äriprotsessi turbeviis tuletatakse määratud kaitsetarbest, mida hinnatakse arvestades konfidentsiaalsuse, tervikluse ja käideldavuse aspekte. Organisatsioonil on võimalik valida turbeviisiks põhiturve, standardturve või tuumikuturve. Punkt on toodud E-ITSi rakendusjuhendis, vastab ka ISO/IEC 27002 kontrollile 5.36 „Vastavus infoturbe poliitikatele, reeglitele ja standarditele" – organisatsiooni infoturbe poliitika, teemakohaste poliitikate, reeglite ja standardite järgimist tuleb regulaarselt üle vaadata.

- Hankija koostab kaitseala struktuurianalüüsi – kaitsetarbe määramisel oleks piisav ettekujutus kaitseala koosseisust ja keerukusest. Kaitseala hulka võivad kuuluda hooned ja ruumid, vajalikud IT-rakendused, klientarvutid, serverid, võrgukomponendid, samuti teenuseandjate poolt pakutavaid IT-teenuseid. Punkt kuulub E-ITSi rakendusjuhendisse.

- Struktuurianalüüsi abil määratletakse sihtobjektide kaitsetarve ning asutakse sihtobjekte modelleerima. Sihtobjektidele määratakse rakendatavad turvameetmed kaitsetarbe alusel. Äriprotsessidele ja teabele esitatud nõuete ning kahjustsenaariumide küsimustiku abil kontrollib hankija kaitsetarbe asjakohasust. Leitav E-ITSi rakendusjuhendist.

- Teenuse turvanõuete määramisel on arvestatud, mis andmeid töödeldakse ning milline peab olema andmevahetusprotseduuride ja -liideste turve. Hea oleks arhitektuurilise joonise olemasolu, ehk milliseid liidestusi peab kaitsma. Väljast tellitava teenuse turvanõuete määramisel on arvestatud äriprotsesside vahelist sõltuvust ning protsesside sisendeid ja väljundeid. Punkt vastab ISO/IEC 27002 kontrollile 5.21 „Infoturbe haldamine IKT tarneahelas" – protsessid ja menetlused tuleks määratleda ning rakendada, et juhtida infoturbega seotud riske, mis on seotud IKT toodete ja teenuste tarneahelaga.

- Hankija viib läbi riskianalüüsi tellitavatele teenusele – riskide kaalutlemise metoodika loomise aluseks on E-ITS riskihaldusjuhend ja E-ITS alusohtude kataloog. Riskianalüüs on vaja läbi viia on läbi tellitavat teenust enam mõjutavate alusohtude lõikes. Punkt vastab E-ITSi rakendusjuhendile ning ISO/IEC 27002 kontrollile 5.19 „Infoturbe tagamine tarnijasuhtes" – protsessid ja menetlused tuleks määratleda ning rakendada, et juhtida infoturbega seotud riske, mis kaasnevad tarnija toodete või teenuste kasutamisega.

- Hankija tuvastab rakendatavad meetmed ning analüüsib, millised on teenuseandja osutada – hankija tutvub vajalike moodulitega, seab need vastavusse hangitava objektiga, tutvub moodulis toodud ohtude nimekirjaga, et aru saada moodulis sisalduvate meetmete eesmärkidest. Vastendab moodulid ja sihtobjektid. Hankija hindab määratud meetme sobivust, teostatavust, piisavust, võimalikku toime efektiivsust ja meetmete omavahelisi mõjusid. Meetmete rakendamise teostatus esitatakse nn „PEARO" põhimõttel (P – Pole asjakohane; E – Ei ole rakendatud; A – Aktsepteeritud risk; R – Rakendatud; O – Osaliselt). Hankija teadvustab ja aktsepteerib jääkriskid. Punkt on pärit E-ITS rakendusjuhendist.

- Hankija otsustab riskianalüüsi ja meetmete modelleerimise tulemusel, millised on rakendatavad meetmed. Punkt on pärit E-ITS rakendusjuhendist. Seejärel määrab hankija, millised meetmed on teenuseandja osutada.

6.2 Kubernetese ja veebiserveri teenustele rakenduvate meetmete analüüs lähtudes vastutaja vaatepunktist koos kommentaaridega

Autor koostas kontrollnimekirjad teenustele Kubernetes ja veebiserver kasutades E-ITSi meetmekataloogis olevaid põhi- ja standardmeetmeid. Autor analüüsis meetmete sisu punktide kaupa andes hinnangu, kes on meetme rakendamise eest vastutav osapool – hankija või teenuseandja. Analüüsi tulemiks on tabelid, mis on koostatud näitena hankijale meetmete rakendamise vastutaja rolli hindamisel. Hinnangud on valideeritud lahenduse arhitektiga kasutades sama põhimõtet ning läbi viidud intervjuude käigus huvitatud osapooltega.

Tabelid koosnevad veergudest:

- E-ITS meede;
- meetmeklass
- meetme nimetus;
- meetme rakendamise eest vastutaja (osaliselt – vastus on teatud meetmete teostamisel hankijal, teenuseandjal või hankija tellitav arendajalt; hankija – hankija vastutus; teenuseandja – teenuseandja vastutus);
- vajadusel meetme rakendamise vastutava osapoole täpsustav kommentaar, kui meede sisaldab rohkem kui ühte tegevust ja tegevused on jaotunud mitme osapoole vahel.

6.2.1 Kubernetes

Kubernetese teenuse hankimisel koostatava tehnilise kirjelduse täpsustamiseks koostab hankija Tabelis 1 olevat arvesse võttes nimekirja sobivatest meetmetest, mis on teenuseandja vastutusalas ja mis on hankija „PEARO" põhimõttel osutunud rakendamist vajavaks meetmeks. Meetmete täitmise hinnangul lähtus autor küsimusest: „Kas seda on võimalik teha teenuseandjal?" Teenuseandja vastutusalasse jäävad meetmed on need, mille võib tuua välja hanke tehnilises kirjelduses ning on õigustatud ootus, et teenuseandja täidab antud nõuded.

Tabel 1 - Kubernetese teenus[4]

E-ITS meede	Meetme-klass	Nimetus	Meetme rakendamise eest vastutaja	Meetme täitmise kommentaar
APP.4.4.M1	Põhi-meede	Rakenduste eraldatuse kavandamine	hankija	hankija koos arendajaga
APP.4.4.M2	Põhi-meede	Rakenduste arenduse automatiseerimine CI/CD abil	mõlemad osapooled	a. teenuseandja b. teenuseandja c. hankijalt tekkivad nõuded
APP.4.4.M3	Põhi-meede	Kubernetese identiteedi- ja õiguste halduse kavandamine	teenuseandja	
APP.4.4.M4	Põhi-meede	Pod’ide eraldamine	teenuseandja	
APP.4.4.M5	Põhi-meede	Klastri andmete varundamine	teenuseandja	
APP.4.4.M6	Standard-meede	Pod’ide turvaline lähtestamine	teenuseandja	võib olla ka arenduspartneri teostada
APP.4.4.M7	Standard-meede	Kubernetese võrkude eraldamine	teenuseandja	
APP.4.4.M8	Standard-meede	Kubernetese konfiguratsioonifailide turve	teenuseandja	
APP.4.4.M9	Standard-meede	Kubernetese teenusekontode turve	teenuseandja	arendus peab toetama, hankija peab tellima
APP.4.4.M10	Standard-meede	Automatiseerimisprotsessi turve	teenuseandja	
APP.4.4.M11	Standard-meede	Konteinerite kasutuse seire	teenuseandja	
APP.4.4.M12	Standard-meede	Taristurakenduste turve	teenuseandja	

[4]https://eits.ria.ee/et/versioon/2023/eits-poohidokumendid/etalonturbe-kataloog/app-rakendused/app4-aerirakendused/app44-kubernetes

Tabelis teenuseandja märgistusega meetmete tulemil tuleb vastu võtta otsus, millised nendest meetmetest saaks viia hanke tehnilisse kirjeldusse.

6.2.2 Veebiserver

Veebiserveri teenuse hankimisel koostatava tehnilise kirjelduse täpsustamiseks koostab hankija Tabelis 2 olevat arvesse võttes nimekirja sobivatest meetmest, mis on teenuseandja vastutusalas ja mis on „PEARO" põhimõttel osutunud rakendamist vajavaks meetmeks. Tabelis on toodud E-ITSi põhi- ja standardmeetmed. Meetmete täitmise hinnangul lähtus autor küsimusest: „Kas seda on võimalik teha teenuseandjal?" Teenuseandja vastutusalasse jäävad meetmed on need, mille võib tuua välja hanke tehnilises kirjelduses ning on õigustatud ootus, et teenuseandja täidab antud nõuded.

Tabel 2 Veebiserveri teenus[5]

E-ITS meede	Meetme-klass	Nimetus	Meetme rakendamise eest vastutaja	Meetme täitmise kommentaar
APP.3.2.M1	Põhi-meede	Veebiserveri turvaline konfigureerimine	mõlemad osapooled	a. teenuseandja b. teenuseandja c. teenuseandja d. teenuseandja e. hankija annab veebirakenduse paigaldusjuhistega
APP.3.2.M2	Põhi-meede	Veebiserveri failide kaitse	mõlemad osapooled	a. teenuseandja b. teenuseandja c. teenuseandja d. rakenduse arendaja vastutab, et oleks kasutatud turvaliselt krüpteeritud salvestust
APP.3.2.M3	Põhi-meede	Failide üles- ja allalaadimise turve	mõlemad osapooled	a. teenuseandja b. teenuseandja c. teenuseandja d. vajab arendaja tuge
APP.3.2.M4	Põhi-meede	Sündmuste logimine	mõlemad osapooled	a. teenuseandja b. sisend arendajalt, et rakendus suudab logi saata ja sellega midagi teha
APP.3.2.M5	Põhi-meede	Autentimine	teenuseandja	

[5]https://eits.ria.ee/et/versioon/2023/eits-poohidokumendid/etalonturbe-kataloog/app-rakendused/app3-voorguteenused/app32-veebiserver

APP.3.2.M7	Põhi-meede	Veebisisu avaldamise õiguspärasus	hankija	
APP.3.2.M11	Põhi-meede	Krüpteerimine TLS abil	teenuseandja	
APP.3.2.M8	Standard-meede	Veebiserveri rakendamise kava	hankija	
APP.3.2.M9	Standard-meede	Veebiserveri turvapoliitika	hankija	
APP.3.2.M10	Standard-meede	Sobiv veebimajutaja	mõlemad	
APP.3.2.M12	Standard-meede	Vigade ja veateadete käsitluse kord	kolmanda osapoole poolt	hankija tellitav arendajalt
APP.3.2.M13	Standard-meede	Veebirobotite juurdepääsu piiramine	teenuseandja	
APP.3.2.M14	Standard-meede	Tervikluse kontroll ja kaitse kahjurvara eest	mõlemad osapooled	a. hankija b. teenuseandja
APP.3.2.M16	Standard-meede	Läbistustestimine ja läbivaatus	hankija	a. hankija tellitav b. hankija vastutav c. hankija vastutav
APP.3.2.M20	Standard-meede	Kontaktisiku määramine	hankija	

Tabelis teenuseandja märgistusega meetmete tulemil tuleb vastu võtta otsus, millised nendest meetmetest saaks viia hanke tehnilisse kirjeldusse.

6.3 Valitud meetmete viimine tehnilisse kirjeldusse ja edasised tegevused

Kubernetese või veebiserveri tabeli infot arvesse võttes otsustab hankija, kas on varasid, mis vajavad täiendavaid meetmed. Meetmete kasutamisvajaduse üleklassifikatsioon võib viia tarbetute meetmete rakendamiseni, mis toob kaasa lisakulud või vastupidi, alaklassifikatsioon võib viia ebapiisavate meetmeteni, et kaitsta informatsiooni kompromiteerimise eest.

Hankija tegevused küberturbe meetmete tehnilise kirjelduse loomiseks:

- kinnitab turvameetmed – kontrollides lisandunud meetmete sobivust infoturbepoliitika ja -eesmärkidega. Vajadusel määrab asendavad turvameetmed neile, mida ei ole võimalik teostada. Hankija hindab mitteteostatavate meetmete põhjustatud jääkriskid. See nõue pärineb E-ITSi rakendusjuhendist.

- Riskiomanikud (protsessijuhid) aktsepteerivad jääriskid. See soovitus pärineb E-ITSi rakendusjuhendist.

- Hankija koostab ülaltoodud tabelite põhjal hangitava objekti tehnilise kirjelduse, milles toob välja meetmed, mida teenuseandja teenust osutades rakendama peab ja mille rakendamise eest vastutab. Antud punkt vastab ISO/IEC 27002 kontrollile 5.20 „Infoturbe käsitlemine tarnijalepingutes" – iga tarnijaga peaks sõltuvalt tarnijasuhte tüübist olema kehtestatud ja kokku lepitud asjakohased infoturbe nõuded.

- Organisatsioon peaks tuvastama äriteenuste ja infosüsteemide käideldavuse nõuded. Organisatsioon peaks kavandama ja rakendama süsteemide arhitektuuri koos vajaliku liiasusega (inglise keeles *redundancy*) nende nõuete täitmiseks. Käideldavuse nõuded on viidud tehniliste nõuete nimekirja. Punkt vastab ISO/IEC 27002 kontrollile 8.14 „Informatsiooni töötlemise rajatiste dubleerimine" – informatsiooni töötlemise rajatised tuleks rakendada piisava dubleerimisega, et vastata käideldavuse nõuetele.

7. Intervjuud

Autor viis läbi ajavahemikus märtsist kuni aprillini intervjuud huvitatud osapooltega – hankijate ja teenuseandjatega, eesmärgiga uurida nende kogemusi seoses erinevate infoturbe standardite rakendamisega nii hangete koostamisel kui ka neile vastamisel. Intervjuude käigus valideeriti kontrollnimekirjade sisu ja saadi vajalikku tagasisidet täpsustuste tegemiseks. Intervjuude ja kontrollnimekirjadele antud hinnangute ülevaade on esitatud käesolevas magistritöö peatükis. Teenuseandjate intervjuude põhjalikum kokkuvõte koos intervjuu küsimustega on esitatud Lisas 3, hankijate intervjuude kokkuvõte koos küsimustega on esitatud Lisas 4.

7.1 Telia Eesti AS

Intervjuu toimumise ajal, 15.03.2024, oli intervjueeritav Telia Eesti AS kliendilahenduste peaarhitekt.

Intervjueeritav tõi esile, et hangete kvaliteet kannatab sageli ebamääraste hanketingimuste kirjelduse all. Ta tõi välja, et hankijate poolt läbiviidavate turu-uuringute puudumine ja lihtsustatud „teenus vastab E-ITSile“ kirjeldused piiravad hangete spektri mõistmist ning võivad kaasa tuua ebarealistlikud ootused hankeobjekti maksumuse ja teostatavuse osas.

Intervjuus käsitleti ka E-ITSi või ISKE standardite tundmise puudumist hankijate seas ning ekspertide vähest kaasatust hankeprotsessis. Intervjueeritav juhtis tähelepanu vajadusele täpsustada hangete tehnilisi kirjeldusi ja parandada standardite mõistmist, mis võib aidata vähendada hankijate ja teenuseandjate vahelisi ebakõlasid. Lisaks tõstis intervjueeritav esile, et standardite, nagu ISO/IEC 27001, parem integreerimine hangetesse võib parandada hankemenetluste kvaliteeti ja selgust. Intervjuus arutleti ka turu-uuringute tähtsuse üle hankemenetluste parema struktureerimise ja läbipaistvuse saavutamiseks, mis aitaks mõlemal poolel paremini mõista hangitava ootusi ja võimalusi.

Autori koostatud kontrollnimekirjade kohta leidis intervjueeritav, et rakenduse arenduse protsess võiks olla omas nimekirjas eespool – äripoole visiooni loomise ajal. Lisamärkusena ütles, et arenduse hangetel võiks kaasata kohe ka tulevast teenuse haldajat, et too saaks anda oma sisendi arendajale anda. Intervjueeritav lisas, et arhitektuuriline joonis liideste kohta võiks samuti hankes kaasas olla – loogiline või protsessiline, kuna see annab ülevaate, mille turvalisust oodatakse.

Intervjueeritava seisukohalt teeb kontrollnimekiri ja selle järgimine hanked kvaliteetsemaks – hankija teadvustab, mida soovib ja teenuseandjal on võimalik täpsemini vastata. Tabelite meetmete vastutaja jagamise loogika märkusena tõi välja, et iga teenus on päeva lõpus natuke oma nägu, on võimatu luua mudel, mis kõigile sobib, kui 80% kattub, on juba väga hästi. Mõlemad tabelid täidavad selle kriteeriumi.

Intervjueeritav rõhutab, et toetavate teenuste puhul tagab teenuseandja rohkem meetmete rakendamist ning lisab, et kui hankija ise ei tea, mida soovib rakendada, siis on teenuseandjal raske vastata. Intervjueeritava arvamuse kohaselt tundub hetkel, et hankijad on mures, kes vastutab ja igaks juhuks kirjeldavad turvameetmeid võimalikult üldsõnaliselt.

7.2 Primend OÜ

Intervjuu Primend OÜ IT-teenuste ärikonsultandiga toimus 27.03.2024. Intervjueeritav toob esile, et hankeprotsessid kipuvad keskenduma madalaimale hinnale, jättes sageli tähelepanuta teenuse kvaliteedi ja teenuseandja kompetentsi. Ta märgib, et hanke dokumentatsioon on tihti aegunud, mis peegeldab puudulikku arusaama kaasaegsest tehnoloogiast ja turvanõuetest. Intervjueeritav rõhutab vajadust keskenduda andmete turvalisusele eriti virtuaalkeskkondades ja pilvteenustes. Intervjueeritav toob esile vajadust turvaintsidentide käsitluse protsesside ajakohastamise järele, et vastata kiiresti areneva IKT-sektori vajadustele.

Intervjueeritav märgib, et ISO/IEC 27001 standardi rakendamine võib pakkuda kuluefektiivset ja rahvusvaheliselt tunnustatud lähenemist turvalisusele, kuid E-ITSi rakendamine on endiselt nõutav teatud teenuste puhul nagu X-tee. Ta juhib tähelepanu E-ITSi ja ISO/IEC 27001 standardi vaheliste suhete ebakindlusele ja tõdeb, et E-ITSi asjakohaste ekspertide, nagu konsultantide ja audiitorite, puudus on probleemiks, eriti arvestades, et E-ITSi auditeerimiseks ei saa kasutada välismaiseid partnereid.

Intervjueeritav lisab, et teenuseandja vastutab oma infrastruktuuri ja protsesside ISO/IEC 27001 standardiga kooskõlastamise eest, märkides, et selline sertifikaat võiks teoreetiliselt katta ka E-ITSi nõuded. Ta rõhutab hankeprotsessi käigus esitatavate täpsustavate küsimuste tähtsust, mis aitavad mõista teenuse vastavust nõuetele.

Autori koostatud kontrollnimekirjade kasutamine IKT-hangete koostamisel lihtsustab intervjueeritava hinnangul vastutuse jaotust ja tegevuste määramist, pakkudes selgust ja hõlpsat mõistmist vastutusalade osas. E-ITSi juurutamine, kuigi finantsiliselt koormav, on põhjendatud, et tagada parimate praktikate järgimine ning vajaliku turvalisuse ja süsteemi uuenduste rakendamine. Seejuures rõhutab intervjueeritav, et vananenud tarkvara ja süsteemide, samuti elutsükli lõpuni jõudnud seadmete kasutamine, nõuab uuendusi, et vastata nüüdisaegsetele turvanõuetele ning E-ITSi järgmise kohustus parandab ETOde küberturvet. Intervjueeritav leiab, et kontrollnimekirjad oleks suureks abiks ega leia, et oleks vaja midagi muuta. Tabelid tunduvad loogilised ja arusaadavad.

7.3 Tietoevry Estonia AS

Intervjuu Tietoevry Estonia AS halduseteenuste osakonnajuhi ja lahenduste arhitektiga toimus 03.04.2024. Intervjuus käsitleti IKT-hangete väljakutseid, keskendudes peamiselt tehniliste kirjelduste ja dokumentatsiooni nõuetele. Intervjueeritavad tõid välja, et hangete tehnilistes kirjeldustes esineb sageli liialt tõlgendamisruumi, eriti seoses E-ITSi meetmete rakendamisega, mis jäetakse ilma konkreetsete juhisteta. Nad märkisid, et selline lähenemine jätab teenuseandjatele palju määramatust ning ei soodusta kvaliteetsete lahenduste pakkumist. Intervjueeritavad rõhutasid ka turu-uuringute vajalikkust, mis aitaksid hankijal paremini mõista turul saadaolevaid lahendusi ja nende vastavust turvanõuetele.

Lisaks kritiseerisid nad vastutuse ebakõlasid hangetes, märkides, et dokumentides pole alati selgelt välja toodud, kellele kuulub vastutus teatud turvameetmete rakendamise eest. Intervjueeritavad rõhutasid ISO/IEC 27001 standardi tähtsust, mis tagab teenuseandjatele rahvusvahelise tunnustuse ja aitab klientidel paremini mõista teenuseandjate vastavust turvanõuetele. Nad tõid välja, et E-ITSi rakendamise ulatus on hangete tehnilises kirjelduses leitavate turvanõuete täpsus tihti puudulik, võib see tekitada segadust nõuete täitmisel.

Intervjueeritavad rõhutavad, kui oluline on hankijatel läbi mõelda ja täpsustada hanke nõuded, et vältida tõlgendamisruumi ja tagada selge vastutusjaotus. Nad toovad välja, et

kontrollnimekirjad ja konkreetselt määratletud vastutusalade läbimine aitab hankijatel paremini mõista, mida nad teenuseandjatelt ootavad, toovad hea näitena välja perearstikeskuste ja kohalike omavalitsuste jaoks loodud profiile. Lahenduse arhitekt kommenteerib Kubernetese tabelit ning tõstatab küsimuse vastutuse kohta tarneprotsessides, kus vastutaja määramine ei ole alati selge ning tarneprotsess võib kuuluda ka arendajale. Samas mõlemad soovitavad kasutada tabeleid, mis aitavad määratleda, kes mille eest vastutab, et hankija saaks selgelt aru, mida on teenuseandjalt õigustatud nõuda.

Intervjueeritavad rõhutavad, et hankija peaks E-ITSi või muude standardite rakendamisel arvestama konkreetsete vastutusaladega ja vajadusel kaasama konsultante, kes aitaksid vastutuse jaotamisel. Nad toovad esile, et vastutuse mõistmine ja harimine toimub sageli töö käigus, eriti konfliktiolukordades, mis sunnib organisatsioone oma lähenemist järgnevateks hangeteks kohandama.

7.4 Tallinna Strateegiakeskus

Intervjuu Tallinna Strateegiakeskuse arvuti ja töökohateenuste sisseostu osakonnajuhiga toimus 05.04.2024. Intervjueeritav sõnas, et kuigi E-ITSi rakendamine on seadusega nõutud, on nende organisatsioon selles vallas alles algusjärgus. Ta tõi välja, et infoturbepoliitikad ja käsikirjad on loodud, samas on praktiline rakendamine keerukas ja palju on veel teha. Ta märkis, et nende viimastes hangetes on viidatud veel ISKE-le. Intervjueeritav tõi esile, et E-ITSi rakendamine nõuab pidevat tähelepanu ja koostööd teenuseandjatega, et tagada turvanõuete täitmine.

Ta arutas ka IKT teenuste sisseostmise protsessi, rõhutades, et tehniliste kirjelduste koostamisel ja hankeprotseduuride kujundamisel on nende organisatsioonis mitu vastutavat rühma. Intervjueeritav tõi esile, et usaldusväärsed teenuseandjad käivitavad tavaliselt teenused nõuetekohaselt ning lisakontrolli vajadus puudub.

Intervjueeritav mainis, et järgmised suuremad hanked, mis tulevad mõne aasta pärast, annavad neile aega E-ITSi täielikult rakendada ja kogemusi koguda. Intervjueeritav rõhutas andmeturbepoliitika ja -meetmete tõhususe tagamiseks vajalikku järjepidevust ja dokumenteerimist ning märkis, et teenuseandjate esitatud turvameetmete küsimused hankele vastates näitavad nende pühendumist nõuete täitmisele.

Kontrollnimekirjade tagasiside – intervjueeritav leiab, et kontrollnimekirjad on väga head ja nendest on kasu. Ta kiitis kasutatavaid nimekirju ja tabeleid, mis aitavad hankeprotsesse struktureerida. Intervjueeritav märkis, et talle meeldib olemasolev ülesehitus, kuid tõi välja, et see tuleb kohandada vastavalt organisatsiooni infoturbe küpsusastmele, mis võib nõuda nimekirjade lühendamist või detailsemaks muutmist sõltuvalt, kui kaugele on hankija jõudnud E-ITSi rakendamisega.

Intervjueeritav tunnistas, et tunneb end justkui teekonnal, kuna E-ITSi täielik rakendamine on veel pooleli. Ta rõhutas, et tabelid on loogilised ja aitavad oluliselt kaasa hangete selgusele ja arusaadavusele, aidates seeläbi tagada, et kõik hankes osalejad mõistaksid nõudeid ja ootusi.

7.5 Riigimetsamajandmise Keskus

Intervjuu Riigimetsamajandamise Keskuse (RMK) infoturbe juhiga toimus 12.04.2024. Intervjueeritav tõi välja, et RMK on ISO/IEC 27001 rakendamise algjärgus ning kuigi infoturbepoliitikad on loodud, on praktikas veel arenguruumi. Ta märkis, et RMK,

riigitulundusasutusena, ei ole varasemalt rakendanud ISKE-t ega muid sarnaseid standardeid, mistõttu on turvameetmete rakendamine hangetes uus väljakutse.

Intervjueeritav käsitles Küberturvalisuse seaduse järgimise uudsust paljudele organisatsioonidele, märkides, et olemasoleva süsteemi täiustamine on lihtsam kui uue loomine. Intervjueeritav tõstis esile problemaatilise kohana erinevates infoturbe standardites, nagu ISO/IEC 27001 ja E-ITS, nõude luua organisatsiooni infoturbe poliitika infoturbeprotsessi rakendamise alguses. Ta leidis, et sellisel juhul luuakse poliitika ilma piisava ettevalmistava tööta, muutes selle üldsõnaliseks ja ebaefektiivseks. Ta rõhutas, et standardite rakendamine on aeganõudev ja keeruline protsess, mis nõuab põhjalikku lähenemist ja tõelist pühendumist.

Intervjueeritav rõhutas ka, et dokumentide loomine peab aitama kaasa reaalsetele muudatustele turbepraktikates, mitte olema ainult formaalsus. Intervjueeritav märkis, et RMK põhitegevuse tõttu järgitakse mitmeid ISO standardeid, samuti on rahvusvahelised partnerid rohkem kursis ISO/IEC 27001 standardiga kui E-ITSiga, mis on vähem tuntud väljaspool Eestit. Ta nõustus, et audiitorite puudus võib tekkida probleemiks seoses kasvava nõudlusega järgida infoturbe standardeid.

Intervjueeritav arutleb, et kontrollnimekirjad, mille kontekst ja vajadus on hästi välja toodud, keskendub siiski ainult kahele teenusele: Kubernetes ja veebiserver. Ta leiab, et üldosa kontrollnimekirjast ei mõju küsimustikuna piisavalt terviklikult. Intervjueeritav täpsustab, et kuigi kontrollnimekirjad on kasulikud, võiks need hõlmata laiemat teenuste spektrit. Ta tõstab esile kontrollnimekirjade potentsiaali selgitada hangete nõudeid selgemalt, et vältida hangete venimist. Intervjueeritav märgib, et nõuete liiga üldsõnaline esitamine võib tekitada teenuseandjates segadust ning neil võib tekkida küsimusi, kuidas nõudeid täpselt täita. Intervjueeritav soovitab, et nimekirjades võiks olla detailsemad kirjeldused nõutavate meetmete osas, sealhulgas millises meetmeklassis need asuvad ja mida täpselt rakendada soovitakse, et tagada suurem selgus ja vastutuse selge jaotumine hangetes.

7.6 Eesti Raudtee

Intervjuu toimus 12.04.2024 Eesti Raudtee IT osakonna juhataja ja infoturbe juhiga. Eesti Raudtee on rakendanud ISO/IEC 27001 standardi kasutamise ning selle haldamise eest vastutab spetsiaalne osakond. Intervjuus selgus, et kuigi sertifikaadi olemasolu on hangetes oluline, toimub tegelik kontroll harva. Eesti Raudtee praegustes hangetes nõutakse teenuseandjatelt ISO/IEC 27001 sertifikaati või selle esitamist aasta jooksul. Mõlemad tõdevad, et hangete turvanõuete ja mittefunktsionaalsete nõuete kirjeldused võivad olla ebapiisavad.

Intervjueeritavad selgitasid, et ISO/IEC 27001 standard lubab teatud meetmete mittetäitmist, kui juhatus on selle heaks kiitnud, kuid eeldab, et vähemalt 80% meetmetest on täidetud. E-ITS nõuab teatud tuumikmeetmete täitmist, kuid võimaldab erijuhtudel ka nende mittetäitmist. Nad rõhutavad, et ISO/IEC 27001 on rahvusvaheliselt tunnustatud ja paindlik, mis on Eesti Raudtee paljude välismaa partnerite tõttu oluline, erinevalt E-ITSist, mis on vähem tuntud ja nõuab suuri investeeringuid partneritele „tõlkimiseks" ja rakendamiseks.

Nad tõid esile, et ISO/IEC 27001 paindlikkus võimaldab standardit kohandada vastavalt tehnoloogia arengule ja organisatsiooni spetsiifikale, pakkudes pikaajalist ja kohandatavat lähenemist turvalisuse tagamisel. Samuti leiab osakonnajuhtaja, et E-ITS on keskendunud traditsioonilistele *on-premise* lahendusele, mis ei pruugi olla piisav kaasaegses IT-maastikus,

kus teenused ja andmed asuvad sageli pilves, tuues kaasa valekindlustunde turvameetmete rakendatusest.

Intervjueeritavad arutlevad kontrollnimekirjade ja nende rakendamise üle turvameetmete osas, viidates erinevatele standarditele ja meetoditele nagu OWASP ja CIS 20 tase kaks. Infoturbe juht näeb, et kontrollnimekirju võiks rakendada lihtsamalt, keskendudes kaitsetarbele ja spetsiifilistele nõuetele. IT osakonna juhataja rõhutab, et vastutusalad hangetes ja teenuste pakkumisel ei pruugi alati olla ilmselged ning toob näiteks: kui lahendus on koostatud kasutades infrastruktuuri kui teenust (IaaS), siis teenuseandjal võib olla ainult piiratud roll.

Intervjueeritavad arutavad ka seda, et teenuseandja ja hankija vastutusalad on tihti segased, mis nõuab mõlemalt poolelt selgete ootuste ja vastutuste määramist. Infoturbe juht leiab, et hankijad peaksid võib-olla kasutama teisi raamistikke. IT osakonna juhataja toonitab, et hankeprotsessis peab olema selge, mida teenuselt oodatakse, et tagada mõlema osapoole vahel usalduslik ja mõistev suhe.

Mõlemad nõustuvad, et kontrollnimekirjade komplekt on kasulik, kui see sisaldab selgeid juhiseid ja auditeerimise õigust, arvestades teenuste eripärasid. IT osakonna juhataja arvab, et kontrollnimekirjad on kasutatavad, kui on nõutud CIS 20-le vastamist, mis aitaks tagada teenuste kvaliteeti ja turvalisust.

Ühtlasi valideeris autor nii Kubernetese kui veebiserveri teenuse tabeleid Telia Eesti AS pideva täiustamise juhiga, kes kinnitas tabelite jaotuse õigsust ja kasutatavust. Ta tõi eraldi välja meetmed Kurberenetse rakenduse blokis mainitud meetmed APP.4.4.M3, kus hankijal on teoreetiliselt võimalus meetme rakendamisel rolli omada, ning APP.4.4.M12, lisades, et Kubernetes ei ole kõvakettaid, kaheldes meetme asjakohasuses. Pideva täiustamise juht märkis, et suures plaanis on lahendus sobilik, kuid täpsemad detailid ei pruugi olla teostatavad, näiteks andmeside krüpteerimine kõigis võrguportides. Pideva täiustamise juht lisas, et tabelite vastutaja määratlemise jätkuks võiks standardi omanik teha võimalusel samasuguse jaotise standardis endas, lisades sellekohase märke meetme kirjeldusse või kataloogi.

Intervjuude kokkuvõttes ilmneb, et nii hankijad kui ka teenuseandjad tajuvad vastutuspiiride ebaselgust ning autori koostatud tabelid aitavad kaasa teadlikkuse tõstmisele. Autori koostatud kontrollnimekirjade komplekti viis autor Telia Eesti kommentaarid, mis puudutasid üldnimekirja punktide järjestust ning RMK täpsustused meetmeklassi kohta. Samas jäi kontrollnimekirjadesse lisamata RMK kommentaar meetmete täitmise viisi kohta, kuna see on hankija ja teenusekohane. Intervjuudest ilmneb erisus mõiste „vastutus“ arusaamisest. Lõhe tekib kohas, kus hankijad usaldavad teenuseandjat pakkuma oma teenust turvaliselt, kuigi turvalisus on kokku lepitud kliendikohase lepingu piires.

Kokkuvõte

Magistritöö käigus anti ülevaade Eesti infoturbe standardi (E-ITS) kasutamisest IKT-teenuste riigihangetes ja koostati parimatest praktikatest koosnev kontrollnimekirjade komplekt hanke tehnilise kirjelduse turbemeetmete määramiseks.

Eesmärgini jõudmiseks kirjeldas autor relevantseid standardeid ja seaduseid ning riigihanke korraldamise põhimõtteid. Samuti uuris autor 2023. aastal avaldatud IKT-teenuseid puudutavaid riigihankeid ning tõi välja näiteid infoturbe meetmete kirjeldamisest hangete dokumentatsioonis, et iseloomustada hetkeolukorda. Autor analüüsis süvitsi kahte hanget andes hinnangu, millised hankija soovitud meetmetest on hankija enda tagada, millistele vastab teenuseandja ning millised peaksid tulenema koostööst teenuseandjaga.

Seejärel koostas autor kontrollnimekirjade komplekti, mis pakub üht võimalikku lahendust hankijatele, võimaldades neil täpsustada hanke tehnilisse kirjeldusse lisatavate E-ITS meetmete kohta käivaid nõudeid. Autor tugines töös esitatud kontrollnimekirjade komplekti koostamisel E-ITSi rakendusjuhendile ja rahvusvahelise standardiorganisatsiooni poolt kujundatud ISO/IEC 27002 kontrollmeetmetele. Töö eesmärgi täitmist valideeriti nii teenuseandjate kui ka hankijatega läbiviidud intervjuude abil. Töö tulemuseks olev kontrollnimekirjade komplekti näidis aitab hankijal koostada hankes nõutavate E-ITS turvameetmete nimekirja ja määratleda vastutusalad.

RIA saab kasutada magistritöö tulemusi, et hinnata, kas teenuseandjaga seotud vastutusalad tuleks E-ITSi moodulites täpsemalt lahti kirjutada. Kontrollnimekirja komplekt illustreerib, kuidas saaks määratleda vastutusalasid olukorras, kus teenust tellitakse väliselt teenuseandjalt. Magistritöös olev kontrollnimekirja näidis käsitles ainult veebiserverit ja Kubernetest, kuid edaspidi saaks kontrollnimekirja laiendada ka teistele teenustele.

Viidatud kirjandus

[1] Riigi Infosüsteemi Amet. Olukord küberruumis: ummistusrünnakute aasta kordus. *Riigi Infosüsteemi Amet: küberturvalisuse aastaraamat 2024*, 2024, lk 9–13. https://www.ria.ee/amet-uudised-ja-kontakt/uudised-pressikontakt/uuringud-ja-analuusid (28.04.2024).

[2] Eesti Infoturbe standard „Rakendusjuhend". https://eits.ria.ee/et/abimaterjalid/rakendusjuhend (11.03.2024).

[3] Eesti infoturbestandard Lisa 1 (30.01.2024), lk 8. *Riigi Teataja I.* https://www.riigiteataja.ee/aktilisa/1300/1202/4006/MKM_m4_lisa1.pdf (01.04.2024).

[4] Küberturvalisuse seadus (06.08.2022). *Riigi Teataja I.* https://www.riigiteataja.ee/akt/K%C3%BCTS (14.10.2023).

[5] Riigi Infosüsteemi Amet. Järelvalve: mitte karistada, vaid aidata. *Riigi Infosüsteemi Amet: küberturvalisuse aastaraamat 2023*, 2023, lk 48–49. https://www.ria.ee/amet-uudised-ja-kontakt/uudised-pressikontakt/uuringud-ja-analuusid (28.01.2024).

[6] Eesti Infoturbe standard „Juhendid ja näidised". https://eits.ria.ee/et/avalehe-menueue/juhendid (14.10.2023).

[7] Eesti Infoturbe standard „OPS.2.1: Väljasttellimine". https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops2-kaeidutoeoed-teenusena/ops21-vaeljasttellimine/3-meetmed (04.02.2024).

[8] Riigi Infosüsteemi Amet. Küberturvalisus on riigikaitse ja sisejulgeoleku osa. *Riigi Infosüsteemi Amet: küberturvalisuse aastaraamat 2023*, 2023 lk 6–7. https://www.ria.ee/amet-uudised-ja-kontakt/uudised-pressikontakt/uuringud-ja-analuusid (28.01.2024).

[9] Riigi Infosüsteemi Amet. E-ITS: miks ja kellele? *Riigi Infosüsteemi Amet: küberturvalisuse aastaraamat 2023*, 2023, lk 54–55. https://www.ria.ee/amet-uudised-ja-kontakt/uudised-pressikontakt/uuringud-ja-analuusid (28.01.2024).

[10] Eesti Infoturbe standard „ISMS. Nõuded". https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/isms-noouded (08.08.2023).

[11] Eesti Infoturbe standard „Tutvustus". https://eits.ria.ee/et/avalehe-menueue/tutvustus/standardist/ (14.10.2023).

[12] Eesti infoturbestandard (21.12.2022). *Riigi Teataja I.* https://www.riigiteataja.ee/akt/121122022034 (08.08.2023).

[13] Võrgu- ja infosüsteemide küberturvalisuse nõuded (13.12.2022). *Riigi Teataja I.* https://www.riigiteataja.ee/akt/113122022030 (Kasutatud 08.08.2023).

[14] Eesti Infoturbe standard „Rakendamine". https://eits.ria.ee/et/avalehe-menueue/kkk/rakendamine/ (10.10.2023).

[15] KPMG Eestis. „E-ITS". https://kpmg.com/ee/et/home/services/advisory/e-its.html (01.04.2024).

[16] Riigi Infosüsteemi Amet. „Eesti infoturbestandard (E-ITS)". https://www.ria.ee/kuberturvalisus/riigi-infoturbe-meetmete-haldus/eesti-infoturbestandard-e-its (01.04.2024).

[17] Eesti Infoturbe standard „Lühijuhend". https://eits.ria.ee/et/versioon/2020vers1/juhendid/luehijuhend/ (01.04.2024).

[18] Riigi Infosüsteemi Amet. „Eesti Infoturbe standard veebileht, Infosüsteemide turvameetmete süsteem ISKE". https://www.ria.ee/kuberturvalisus/riigi-infoturbe-meetmete-haldus/infosusteemide-turvameetmete-susteem-iske (07.08.2023).

[19] Riigi Infosüsteemi Amet. ISKE rakendusjuhend 8.00, 2017, lk 3–10. https://www.ria.ee/sites/default/files/documents/2022-11/ISKE-rakendusjuhend-8.00.pdf (07.08.2023).

[20] Infosüsteemide turvameetmete süsteem (2007). *Riigi Teataja I.* https://www.riigiteataja.ee/akt/13125331 (02.04.2024).

[21] Eesti Infoturbe standard. „Üleminekujuhend ISKE-lt E-ITSile". https://eits.ria.ee/et/versioon/2020vers1/juhendid/ueleminekujuhend-iskelt-eitsile/#11mismuutubuuestandardiga2 (02.04.2024).

[22] Riigi Infosüsteemi Amet. Infosüsteemide kolmeastmelise etalonturbe süsteem ISKE, Rakendusjuhend, ISKE rakendusjuhendi lisa 1: Kataloogid B, M ja H, 2018, lk 3–40. https://www.ria.ee/sites/default/files/documents/2022-11/ISKE-meetmed-8-00.pdf (08.08.2023).

[23] Majandus- ja Kommunikatsiooniministeerium. KÜBERTURVALISUSE STRATEEGIA 2019–2022. https://www.mkm.ee/sites/default/files/documents/2022-03/kuberturvalisuse_strateegia_2019-2022_0.pdf (03.04.2023).

[24] International Organization for Standardization. „ISO/IEC 27001:2022". https://www.iso.org/standard/27001 (07.08.2023).

[25] International Organization for Standardization. INTERNATIONAL STANDARD ISO/IEC 27002 Information security, cybersecurity and privacy protection — Information security controls. Third Edition. The International Organization for Standardization and the International Electrotechnical Commission, 2022. (04.02.2024).

[26] International Organization for Standardization. „ISO/IEC 27002:2022". https://www.iso.org/standard/75652.html (29.04.2024).

[27] Federal Office for Information Security. IT-Grundschutz-Compendium Edition 2022, Federal Office for Information Security (BSI), 2022, lk 10. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.html (12.04.2024).

[28] Federal Office for Information Security. „IT-Grundschutz". https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (08.08.2023).

[29] Federal Office for Information Security. BSI-Standard 200-2 IT-Grundschutz methodology. Federal Office for Information Security (BSI), 2017, lk 12–13. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.pdf?__blob=publicationFile&v=2 (30.10.2023).

[30] Hädaolukorra seadus (17.05.2020). *Riigi Teataja I.* https://www.riigiteataja.ee/akt/117052020003 (03.12.2023).

[31] Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel (09.01.2024). *Riigi Teataja I.* https://www.riigiteataja.ee/akt/109012024025 (13.04.2024).

[32] Riigihangete seadus (06.07.2023). *Riigi Teataja I.* https://www.riigiteataja.ee/akt/106072023078?leiaKehtiv (07.02.2024).

[33] Pungas, K. Riigihangetega seotud protsessid organisatsioonis. *Grant Thornton Baltic OÜ,* 2016. https://www.grantthornton.ee/insights-landing-page/riigihangetega-seotud-protsessid-organisatsioonis/ (11.02.2024).

[34] Riigihangete register, riigihange nr 265701 „IKT-halduse teenus Türi Vallavalitsusele". 2023. https://riigihanked.riik.ee/rhr-web/#/procurement/5999281/documents/source-document?group=B&documentOldId=16359003 (17.07.2023).

[35] Riigihangete register, riigihange nr 261941 „Turbekeskus teenusena". 2023. https://riigihanked.riik.ee/rhr-web/#/procurement/5662800/general-info (17.07.2023).

[36] Riigihangete register, riigihange nr 262655 „Tallinna sporditegevuse toetuste infosüsteemi arendus-, hooldus- ja majutusteenus". 2023. https://riigihanked.riik.ee/rhr-web/#/procurement/5728140/general-info (17.07.2023).

[37] Riigihangete register, riigihange nr 260642 „Juhtimistarkvara kasutusõiguse teenuse tellimine". 2023. https://riigihanked.riik.ee/rhr-web/#/procurement/5549360/general-info (21.07.2023)

[38] Riigihangete register, riigihange nr 262134 „Andmesideteenus Tallinna hallatavatele asutustele". 2023. https://riigihanked.riik.ee/rhr-web/#/procurement/5682880/general-info (21.07.2023).

[39] Riigihangete register, riigihange nr 269727 „KEMIT Postgre andmebaasi majutusteenus 2024–2028". 2023. https://riigihanked.riik.ee/rhr-web/#/procurement/6374304/general-info (13.01.2024).

[40] Riigihangete register, riigihange nr 261329 „Infosüsteemide majutusteenuse tellimine". 2023. https://riigihanked.riik.ee/rhr-web/#/procurement/5604860/documents/source-document?group=B&documentOldId=16307377 (07.02.2024).

Lisa 1 – Riigihanke „KEMIT Postgre andmebaasi majutusteenus 2024–2028“ detailne analüüs

Lisa 1 on välja toodud detailne analüüs, lähtudes meetmetest, kuidas jaguneb vastutus meetmete kaupa hankija, teenuseandja või hankija ja teenuseandja ühise vastutajana. Analüüsis on lähtutud E-ITSi 2022 versioonist, kuna see oli ka hankes nõutud. Vastutaja jaotus põhineb autori hinnangul vastates küsimusele: „Kas seda saab teenuseandja toetada?“

Hankedokument kirjeldab teenust, mis käsitleb PostgreSQL andmebaaside majutamist ja haldamist, kirjeldades hetkeolukorda ning andes hinnangu hankija puudulikust piisavast kompetentsist PostgreSQLi osas ning on edastab soovi majutada osaliselt baasid teenuseandja juurde, kasutades teenuseandja kompetentse halduse osas. Hankijal on umbes 250 PostgreSQL andmebaasi, enamik neist on alla 200GB suurused. Samuti on kirjeldatud soovitud teenusekäideldavuse nõuded (SLA) ja ressurusinõuded ning eeldatav andmebaaside haldamise aeg kuus.

Üldnõuetes on toodud nõuded teenuseandja ISO/E-ITS standardite järgmiseks, mis on seotud hangitava teenusega. Hankija lisab, et pakutav teenus peab vastama nimetatud E-ITS põhi- ja standardmeetmetele. Samuti peab teenuseandja tagama teenuse turvalisuse ja ajakohasuse.
Hoone ja ruumi (INF. Taristu):
INF.1: Hoone üldiselt
INF.2: Serveriruum ja andmekeskus
INF.5: Tehnilise taristu ruum või kapp
INF.6: Andmekandjate arhiiv
INF.12: Kaabeldus
INF.13: Hoonete tehniline haldus
Võrk (NET. Võrgud ja side):
NET.1.1: Võrgu arhitektuur ja lahendus
NET 1.2: Võrguhaldus
NET.3.1: Ruuter ja kommutaator (KM: M26)
NET.3.2: Tulemüür
Server (SYS. IT-süsteemid):
SYS.1.1: Server üldiselt
SYS.1.2: Windows Server
SYS.1.3: Linuxi ja Unixi server
SYS.1.5: Virtualiseerimissüsteem
SYS.1.6: Konteinerdus
SYS.1.8: Salvestilahendused
Klientarvuti (SYS.2 Klientarvuti kasutamine)
SYS.2.1: Klientarvuti üldiselt
SYS.2.2: Windows kliendid
SYS.2.3: Linuxi ja Unixi klient
SYS.2.4: macOS-i klient
Rakendused ja andmebaasid (APP. Rakendused)
APP.4.3: Andmebaasisüsteemid
Infoturve ja andmevahetus (CON. Kontseptsioonid ja metoodikad)
CON.2: Isikuandmete kaitse
CON.3: Andmevarunduse kontseptsioon
Õiguste haldus ja ligipääsud (ORP. Organisatsioon ja personal):
ORP.4: Identiteedi- ja õiguste haldus
Andmebaasi kasutamine (OPS. Käidutööd):

OPS.1.1.2: IT-haldus
OPS.1.1.3: Paiga- ja muudatusehaldus
OPS.1.1.5: Logimine
OPS.1.1.6: Tarkvara testimine ja kasutuselevõtt
OPS.1.1.7: Süsteemihaldus
OPS.2.1: Väljasttellimine
OPS.2.2: Pilvteenuste kasutamine
OPS.3.1: Teenuseandja infoturve

Hangitava teenuse nõuded juurkasutaja (inglise keeles *Superuser*) vaates välistavad teenuseandja täiskontrolli. See tähendab, et hankija vastutab suuresti oma andmebaaside halduse eest, kuigi teenuseandja võib pakkuda tuge ja infrastruktuuri.

Hankija soovitud teenuse, PostgreSQL andmebaaside majutuse ja halduse, kontekstis ei pruugi kõik mainitud E-ITS moodulid olla võrdselt olulised või vajalikud. PostgreSQL andmebaaside majutuse ja haldusega on autori hinnangul otseselt seotud järgmised hankes mainitud moodulid:

- Hoone ja ruumi turvalisus (INF): oluline andmekeskuste ja serveriruumide puhul, kus PostgreSQL andmebaase majutatakse. See tagab füüsilise turvalisuse;
- võrguturvalisus (NET): väga oluline, kuna andmebaasid peavad olema kaitstud võrgupõhiste rünnakute ja nõrkuste eest, eriti kui andmebaasid on kättesaadavad üle võrgu;
- serverite ja süsteemide turvalisus (SYS): otseselt seotud andmebaaside majutamisega, kuna need nõuded tagavad serverite ja operatsioonisüsteemide turvalisuse, kus andmebaase hoitakse;
- rakenduste ja andmebaaside turvalisus (APP): eriti oluline moodul, kuna see käsitleb konkreetselt andmebaasisüsteemide turvalisust;
- infoturve ja andmevahetus (CON): oluline andmete kaitse ja varundamise seisukohast, tagades, et andmeid hoitakse turvaliselt ja taastatakse efektiivselt hädaolukorras;
- õiguste haldus ja ligipääsud (ORP): vajalik andmebaaside haldamisel, et tagada ainult volitatud isikute ligipääs andmebaasidele;
- andmebaasi kasutamine ja haldus (OPS): otseselt seotud PostgreSQL andmebaaside haldusega, hõlmates IT-haldust, logimist ja süsteemihaldust.

Teised moodulid, nagu klientarvutite turvalisus, võivad olla vähem olulised, kui need ei puutu otseselt kokku andmebaaside majutuse ja haldusega.

Hanke ülejäänud punktid täpsustavad nõudeid andmekeskusele, andmekeskuste füüsilistele ligipääsudele, turvalisuse ja andmekaitsele, varundusele ja andmetaastele, klienditoele ja monitooringule.

Vaatleme lähemalt soovitud E-ITSi moodulitele vastutaja jaotust.
Hoone ja ruumi (INF. Taristu)[6] – serveriruumi ja andmekeskusega seonduvate meetmete täitmise eest vastutab IT-talitus
INF.1: Hoone üldiselt – kõikide E-ITSi meetmete rakendamise eest E-TSi vastutab teenuseandja.

[6] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/inf-taristu/inf1-hoone-ueldiselt

INF.2: Serveriruum ja andmekeskus – kõikide E-ITSi meetmete rakendamise eest E-TSi vastutab teenuseandja.
INF.5: Tehnilise taristu ruum või kapp – kõikide E-ITSi meetmete rakendamise eest E-TSi vastutab teenuseandja.
INF.6: Andmekandjate arhiiv – arhiveerimine ei ole relevantne seoses kõnealuse hankega.
INF.12: Kaabeldus – kõikide E-ITSi meetmete rakendamise eest E-TSi vastutab teenuseandja.
INF.13: Hoonete tehniline haldus – kõikide E-ITSi meetmete rakendamise eest E-TSi vastutab teenuseandja.

Võrk (NET. Võrgud ja side)[7] – võrgu arhitektuuri ja võrgulahenduse infoturbe meetmed, võrgu arhitektuuri ja võrgulahenduse meetmete täitmise eest vastutab arhitekt
Hankija kohustused:
NET.1.1: Võrgu arhitektuur ja lahendus – kuigi andmekeskus tagab füüsilise ja võrgu tasandi kaitse, on hankija kohustus ise välja töötada ja kehtestada oma võrgu turvapoliitika, mis on kooskõlas organisatsiooni üldise infoturvapoliitikaga ja kajastab võrgule omaseid vajadusi.
NET.1.1.M2: Võrgu dokumentatsioon – hankija dokumenteerib oma sisevõrgu struktuuri ja muudatused selles, samuti kuidas võrgu ülesehitus on korrelatsioonis välise majutusteenusega.
NET.1.1.M3: Võrgu tehniliste nõuete spetsifitseerimine – hankija koostab, uuendab vastavalt turvapoliitika või ärivajaduse muudatusele võrgu tehnilised nõuded. Teostus võib tulla teenuseandjalt, kes peab juhendeid järgima.
NET.1.1.M10: Demilitaartsoon – hankija kehtestab demilitaartsoonide kasutamise korra vastavalt IT-süsteemide ja andmete kaitsetarbele.
NET.1.1.M15: Võrgu vastavuskontroll – hankija kontrollib võrgu vastavust loodud turvapoliitikale ning omab kriteeriumeid, millele lähtub kontrollimisel.
NET.1.1.M16: Võrgu arhitektuuri dokumenteerimine – hankija dokumenteerib ja hoiab ajakohasena oma sisemise võrgu arhitektuuri, sealhulgas kuidas see integreerub välise majutusteenusega.
NET.1.1.M17: Võrgulahenduse spetsifitseerimine – hankija on koostanud tehnilise lahenduse kava ja tagab, et kõik turvameetmed ja võrgu disain vastavad kehtivatele nõuetele ja organisatsiooni turvapoliitikale. Võib nõuda koostööd teenuseandjaga, kui võrgulahenduse rakendamine hõlmab kolmandate osapoolte tehnoloogiaid või teenuseid. Hankija tagab, et teenuseandja panus on kooskõlas organisatsiooni turvapoliitika, tehniliste nõuete ja äriliste eesmärkidega.
NET.1.1.M22: Segmentimise eeskiri – hankija koostab võrgu segmenteerimise eeskirja, kus on kirjeldatud võrgusegmentide kavandamine, uute segmentide loomine ja lõppseadmete paigutamine, mis on kooskõlas organisatsiooni äriprotsesside ja turvanõuetega. Hankija vastutab turvapoliitika ja -praktika oleksid järjepidevuse eest.
NET.1.1.M25: Võrgu arhitektuuri ja võrgulahenduse detailplaneerimine – hankija koostab võrgu arhitektuuri ja võrgulahenduse jaoks detailse teostusplaani.
NET.1.1.M26: Võrgu käitusjuhend – hankija töötab välja ning järgib võrgu käitusjuhendit, mis kirjeldab organisatsiooni siseseid võrgu haldamise protseduure.
NET.1.1.M27: Võrgu arhitektuuri arvestamine avariivalmenduses – hankija tagab, et kõik muudatused võrgu arhitektuuris oleksid kooskõlas avariivalmiduse nõuetega ega vähendaks organisatsiooni võimet taastuda IT-süsteemide rikete või katastroofide korral.
Teenuseandja kohustused:

[7] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/net-voorgud-ja-side/net1-voorgud-ja-side/net11-voorgu-arhitektuur-ja-lahendus/3-meetmed/

NET.1.1.M4: Võrgu tsoneerimine – teenuseandja tagab, et võrk on füüsiliselt jagatud tsoonideks, et piirata ligipääsu teatud võrguosadele vastavalt nende turvavajadustele ja -funktsionaalsusele.
NET.1.1.M5: Klientide ja serverite võrgusegmentide eraldamine – teenuseandja kohustub hoidma kliente ja teenuseid pakkuvaid servereid eraldi võrgusegmentides.
NET.1.1.M6: Lõppseadmete segmendid sisevõrgus – teenuseandja jagab lõppseadmed samasse võrgusegmenti vastavalt nende turbevajadusele.
NET.1.1.M7: Tundliku teabe turve võrgus – teenuseandja kasutab andmete edastamisel ajakohaseid ja turvalisi võrguprotokolle või usaldusväärseid ning turvatud sidekanaleid
NET.1.1.M8: Internetti pääsu alusturve – teenuseandja suunab internetiliikluse läbi tulemüüri, mis filtreerib liiklust protokolle ja võrguühendusi piiravate tulemüürireeglite alusel. Peab olema hankija tellitud.
NET.1.1.M9: Turvaline andmevahetus ebausaldusväärsete võrkudega – teenuseandja määrab iga andmeid vahetava võrgu jaoks usalduvustaseme.
NET.1.1.M11: Siseneva andmeliikluse turve – teenuseandja tagab, et pääs välistelt IP-aadressidelt sisevõrku toimub läbi suunatud turvalise sidekanali.
NET.1.1.M12: Väljuva andmeliikluse turve – teenuseandja suunab sisevõrgust Internetti suunduvad andmed läbi väljaspool sisevõrku asuva turvaproksi või vastavat võimekust omava keskse tulemüüri.
NET.1.1.M18: Internetiühenduse P-A-P-struktuuri (paketifilter-rakenduslüüs-paketifilter) kasutamine – teenuseandja tagab Internetiühenduse P-A-P-struktuuri kasutamise, rakendades kahetasemelist tulemüürisüsteemi.
NET.1.1.M19: Taristuteenuste eraldamine – teenuseandja tagab, et IT-taristule baasteenuseid osutavad serverid asuvad eraldatud võrgusegmendis ning andmeside on kaitstud dünaamilise paketifiltriga.
NET.1.1.M20: Alamvõrgud IPv4/IPv6 lõppseadmetele – teenuseandja jagab lõppseadmed alamvõrkudesse vastavalt sellele, kas seadmed kasutavad IPv4, IPv6 või mõlemat protokolli.
NET.1.1.M21: Haldusvõrkude eraldamine – teenuseandja tagab, et võrgutaristu halduseks kasutatakse üldisest andmesidest eraldatud sidekanalit ning haldustööjaamad asuvad eraldi võrgusegmentides.
NET.1.1.M23: Võrgusegmentide eraldamine – teenuseandja tagab, et erinev kaitsetarbega IT-süsteemid asuvad erineva turvatasemega võrgusegmentides, kui see on hankija poolt tellitud.
NET.1.1.M24: Võrkude loogiline eraldamine VLAN-iga – teenuseandja tagab võrkude loogilise eraldamise VLAN-i abil.

Ühised kohustused:

NET.1.1.M13: Hankija koostab võrgu teostuskava vastavalt turvapoliitikale ja nõuetele, teenuseandja tagab, et võrgu ehitamine ja haldamine vastab turvanõuetele.
NET.1.1.M14: Võrgu kavakohane teostus – hankija kontrollib teenuseandja rajatud võrgu vastavaust teostuskavale.
NET.1.1.M26: Võrgu käitusjuhend – hankija töötab välja ning teenuseandja järgib võrgu käitusjuhendit, mis kirjeldab organisatsiooni siseseid võrgu haldamise protseduure.

NET 1.2: Võrguhaldus[8] – meetmed turvalise võrguhalduse rajamiseks ja käigus hoidmiseks ning turvalise andmeside tagamiseks, meetmete täitmise eest vastutab IT-talitus

Hankija kohustused:

[8] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/net-voorgud-ja-side/net1-voorgud-ja-side/net-12-voorguhaldus/3-meetmed/

NET.1.2.M1: Võrguhalduse kavandamine – hankija kavandab võrguhalduse, lähtudes oma infoturvapoliitikast ja erivajadustest.
NET.1.2.M2: Võrguhalduse nõuete spetsifitseerimine – hankija dokumenteerib võrguhaldusele kehtestatud nõuded, veendudes, et need on kooskõlas organisatsiooni turvapoliitika ja ärivajadustega.
NET.1.2.M11: Võrguhalduse juhend – hankija koostab võrguhalduse juhendi, mis katab kasutatavad võrguteenused ja -haldusvahendid ning meetmed võrguhaldustegevusteks, logimiseks ja andmeside turbeks ning kontrollib selle järgimist.
NET.1.2.M13: Võrguhalduse kontseptsioon – hankija töötab välja võrguhalduse kontseptsiooni, mis hõlmab meetodeid, tehnoloogiaid ja turvanõudeid vastamaks organisatsiooni vajadustele.
NET.1.2.M14: Võrguhalduse rakendusplaan – hankija koostab võrguhalduse rakendusplaani ning vastutab selle eest, et võrguhalduse kontseptsioon ja juhendid oleksid kooskõlas organisatsiooni üldiste eesmärkide ja poliitikatega.
NET.1.2.M15: Võrguhalduse taristu turvalise kasutamise kord – turvalise kasutamise kord on välja töötatud lähtuvalt võrgu turvapoliitikast ja peab olema kooskõlas organisatsiooni üldiste turvanõuetega.
NET.1.2.M17: Regulaarne võrguhalduse ülevaatus – hankija kontrollib regulaarselt võrguhaldusele esitatud nõuete ja dokumentatsiooni vastavust.
NET.1.2.M27: Võrguhalduse avariivalmendus – hankija integreerib võrguhalduse avariivalmenduse oma üldisesse avariivalmenduse plaani.

Teenuseandja kohustused:

NET.1.2.M6: Regulaarne andmevarundus – teenuseandja vastutab andmete regulaarse varundamise eest.
NET.1.2.M8: Kellaaja sünkroniseerimine – teenuseandja tagab kellaaegade sünkroniseerimise.
NET.1.2.M9: Võrguhalduse side turve – teenuseandja vastutab võrguhalduse andmeside turvalisuse eest.
NET.1.2.M10: SNMP-side piiramine – teenuseandja vastutab SNMP protokolli kasutamise piiramise eest.
NET.1.2.M12: Võrguhalduse dokumenteerimine – teenuseandja vastutab võrguhalduse dokumentatsiooni eest.
NET.1.2.M16: Võrguhalduslahenduste turvaline konfigureerimine – teenuseandja vastutab turvalise konfigureerimise eest.
NET.1.2.M18: Võrguhalduse koolitus – teenuseandja vastutab võrguhalduse koolituse eest, tagades töötajate pädevuse ja teadlikkuse turvanõuetest.
NET.1.2.M21: Võrguhalduse side lahusus – teenuseandja vastutab halduspääsu piiramise eest, et vältida volitamata ligipääsu võrgukomponentidele ning kaitsta võrgu turvalisust.
NET.1.2.M22: Haldusfunktsioonide piiramine – teenuseandja vastutab haldusfunktsioonide piiramise eest.
NET.1.2.M24: Võrgukomponentide keskne konfiguratsioonihaldus – teenuseandja vastutab keskse konfiguratsioonihalduse eest, see tagab võrgukomponentide ühtlase ja turvalise konfigureerimise ning reageerib muudatustele ja probleemidele.
NET.1.2.M25: Võrgukomponentide seire – teenuseandja vastutab võrgukomponentide seire eest, et kiirelt reageerimida võimalikele rikketele või turvarikkumistele.
NET.1.2.M26: Sündmuste teavitus, alarmeerimine ja logimine – teenuseandja vastutab sündmuste logimise ja teavitamise eest.
NET.1.2.M28: Haldustööjaamade turvaline paigutus ainukanaliga halduse puhul – teenuseandja peab tagama haldustööjaamade turvalise paigutuse.
NET.1.2.M29: Virtuaalsed kohtvõrgud (VLAN) haldustsoonis – teenuseandja kasutab virtuaalseid haldusvõrke, et tagada võrgu segmenteerimise ja isolatsiooni.

Ühised kohustused:
NET.1.2.M7: Sündmuste logimine – hankija tagab, et tema võrgus toimuvad olulised sündmused (näiteks volitamata pääsukatsed või seadistuste muudatused) logitakse. Teenuseandja võib osutada logimisteenuseid, kuid hankija määrab, millised sündmused on logimiseks olulised.

NET.3.1: Ruuter ja kommutaator[9] – meetmed ruuterite ja kommutaatorite turvaliseks käituseks, meetmete rakendamise eest vastutab IT-talitus
Hankija kohustused:
NET.3.1.M4: Ruuteri või kommutaatori haldusliideste turve – teenuseandja võib pakkuda turvalisi võrguhaldusliideseid, kuid hankija tagab oma võrguseadmete haldusliideste turvalisuse.
NET.3.1.M9: Ruuteri või kommutaatori käidudokumentatsioon – hankija koostab ja haldab kasutusel olevate võrguseadmete käidudokumentatsiooni.
NET.3.1.M10: Ruuterite ja kommutaatorite turvajuhend – võib kattuda teenuseandja pakutavate juhistega, samas hankija tagab seadmete turvajuhendi vastavalt organisatsiooni turvapoliitikale ja järgimise.
NET.3.1.M11: Ruuteri või kommutaatori valimine – hankija vastutab seadmete valiku eest (kehtestab nõuded) oma võrgus, mis on kooskõlas organisatsiooni turvapoliitikaga.
NET.3.1.M21: Pääsuõiguste ja identiteedi haldus võrgutaristus – hankija haldab oma võrguseadmete pääsuõiguste ja identiteedi haldust.
Teenuseandja kohustused:
NET.3.1.M5: Kaitse IP-pakettide fragmenteerimisrünnete eest – teenuseandja tagab ruuterite ja kommutaatoritel oleks turvamehhanismide aktiveerimise, et tõrjuda IPv4- ja IPv6-fragmenteerimisrünnete tõrjeks.
NET.3.1.M7: Ruuterite ja kommutaatorite logimine – teenuseandja logib ruuterite ja kommutaatorite sündmused, sealhulgas konfiguratsiooni muudatused, taaskäivitused, süsteemi tõrked ja muud olulised sündmused.
NET.3.1.M8: Regulaarne andmevarundus – teenuseandja vastutab ruuterite ja kommutaatorite konfiguratsioonifailidele regulaarse andmevarunduse eest.
NET.3.1.M12: Konfiguratsiooni kontroll-loend – teenuseandja koostab ruuterite ja kommutaatorite jaoks konfiguratsiooni kontroll-loendi oluliste turvaseadete kontrollimiseks.
NET.3.1.M13: Eraldatud haldusvõrk – teenuseandja vastutab ruuterite ja kommutaatorite haldamise eest eraldatud haldusvõrgu kaudu, ühtlasi vastutab ka haldusliideste ja -ühenduste kaitsmise eest eraldi tulemüüri abil.
NET.3.1.M14: ICMP-sõnumite kaitsmine väärkasutuse eest – teenuseandja filtreerib ICMP ja ICMPv6 sõnumeid, et väärkasutust tõkestada.
NET.3.1.M15: Võltsitud pakettide ja teeskluse tõkestamine – teenuseandja blokeerib juurdepääsu määramata IP-aadressidelt ruuteritesse ja kommutaatoritesse.
NET.3.1.M16: IPv6 „routing header type 0“ rünnete takistamine – teenuseandja rakendab turvamehhanismid, mis avastavad ja takistavad IPv6 põhinevaid ründeid ruuterites.
NET.3.1.M17: Ummistusrünnete tõrje – teenuseandja rakendab turvamehhanismid, mis avastavad ja tõrjuvad sõnumite suure hulgaga seotud ründeid ning TCP olekukurnamisrünnakuid.
NET.3.1.M18: Pääsuloendid – teenuseandja piirab juurdepääsu ruuteritele ja kommutaatoritele pääsuloendite abil.

[9] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/net-voorgud-ja-side/net3-voorgukomponendid/net31-ruuter-ja-kommutaator/3-meetmed/

NET.3.1.M19: Kommutaatori portide turve – teenuseandja vastutab kommutaatori pordi füüsilise juurdepääsu kaitsmise eest, kui kommutaator asub teenuseandja perimeetris.
NET.3.1.M20: Turvalised marsruutimisprotokollid – teenuseandja tahab marsruutimisandmete vahetamise turvalisuse.
NET.3.1.M23: Läbivaatused ja läbistustestimised – teenuseandja kohustus on regulaarselt kontrollida ja testida ruutereid ja kommutaatoreid teadaolevate turvaprobleemide suhtes ning dokumenteerida läbivaatuste ja läbistustestimiste tulemused.

Ühised kohustused:

NET.3.1.M1: Ruuteri või kommutaatori turvaline baaskonfiguratsioon – hankija määratleb turvanõuded ja poliitikad, teenuseandja teostab vajalikud tehnilised sammud nende nõuete rakendamiseks.
NET.3.1.M6: Ruuteri või kommutaatori avariijuurdepääs – hankija tagab oma võrguseadmetele avariijuurdepääsu, teenuseandja pakub analoogseid lahendusi oma infrastruktuuris.
NET.3.1.M22: Ruuterite ja kommutaatorite avariivalmendus – hankija tagab, et avariivalmenduse plaan oleks koostatud ja integreeritud organisatsiooni üldisesse avariivalmiduse strateegiasse. Osa avariivalmendusega seotud operatiivülesandeid, nagu näiteks ruuterite ja kommutaatorite füüsilist ja tarkvaralist haldust, sealhulgas turvaparanduste rakendamist ja konfiguratsioonimuudatuste tegemist, rikkeotsingu teostamist vastavalt juhendile, saab delegeerida teenuseandjale.
NET.3.1.M26: Kõrgkäideldavuse tagamine – hankija ja teenuseandja tagavad oma võrguseadmete kõrgkäideldavuse.

NET.3.2: Tulemüür[10] – meetmed tulemüüri või tulemüürisüsteemi turvaliseks hankimiseks, rajamiseks, konfigureerimiseks ja käitamiseks, turvameetmete täitmise eest vastutab IT-talitus

Hankija kohustused:

NET.3.2.M7: Tulemüüri avariijuurdepääs – hankija on teadlik protsessidest ja võimalustest avariijuurdepääsuks, teenuseandjale on tagatud võimalus füüsiliseks juurdepääsuks.
NET.3.2.M15: Tulemüüri hankimise kord – hankija määratleb tulemüüri valiku nõuded, mis on kooskõlas organisatsiooni infoturbepoliitikaga.
NET.3.2.M32: Tulemüüri avariivalmendus – hankija integreerib tulemüüri avariivalmenduse oma üldisesse avariivalmenduse plaani.

Teenuseandja kohustused:

NET.3.2.M6: Tulemüüri haldusliideste turve – teenuseandja vastutab, et tulemüüri haldusliidestele oleks võimalik ligi pääseda ainult määratud IP-aadressidelt või -vahemikust ning et haldusliidestele ei oleks juurdepääsu ebausaldusväärsetest võrkudest. Lisaks tagab teenuseandja, et tulemüüri kohtvõrgu haldusühenduste protokollid on turvalised või kasutatakse alternatiivina eraldi haldusvõrku.
NET.3.2.M9: Tulemüüri logimine – teenuseandja logib tulemüüri olulised turvasündmused, sealhulgas haldusliidesesse sisselogimised, konfiguratsioonimuudatused, blokeeritud võrguühendustaotlused, ebaõnnestunud juurdepääsukatsed süsteemiressurssidele ning tulemüüriteenuste ja üldiste tulemüüri veateadete salvestused. Tulemüüri tehtud toimingud logitakse võimalusel automaatselt.
NET.3.2.M10: Killuründe tõrje paketifiltris – teenuseandja tõrjub IPv4 ja IPv6 protokollide killuründe paketifiltris.

[10] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/net-voorgud-ja-side/net3-voorgukomponendid/net32-tulemueuer/3-meetmed/

NET.3.2.M22: Tulemüüri kellaaja sünkroniseerimine – teenuseandja sünkroniseerib tulemüüri kellaaja turvalise NTP-serveriga ning blokeerib kellaaja sünkroniseerimise muude väliste allikatega.
NET.3.2.M16: Turvaline P-A-P-struktuur (paketifilter-rakenduslüüs-paketifilter) – teenuseandja rajab turvalise P-A-P-struktuuri.
NET.3.2.M17: IPv4 või IPv6 desaktiveerimine – teenuseandja desaktiveerib IPv4 või IPv6 protokolli tulemüüri liideses, kui vastav protokoll ei ole võrgusegmendis kasutusel.
NET.3.2.M18: Tulemüüri haldusvõrgu eraldamine – teenuseandja korraldab tulemüüri haldamine eraldi haldusvõrgu kaudu.
NET.3.2.M19: UDP-tulva ja TCP SYN-tulva ning järjenumbri äraarvamise tõrje paketifiltris – teenuseandja vastutab UDP-tulva ja TCP SYN-tulva ning järjenumbri äraarvamise tõrje eest paketifiltris, kasutades paketifiltrit.
NET.3.2.M23: Tulemüüri seire ja seiretulemuste analüüs – teenuseandja vastutab tulemüüri seire ja seiretulemuste analüüsi eest, hõlmates tulemüüride jälgimist, logide analüüsi ning automaatse teavitamise seadistamist oluliste sündmuste korral.
NET.3.2.M24: Läbivaatused ja läbistustestimised – teenuseandja vaatab tulemüüri regulaarselt läbi ja testib teadaolevate turvaprobleemide suhtes ning dokumenteerib läbivaatuste tulemused, et tagada tulemüüri turvalisus ja vastavus turvanõuetele.

Ühised kohustused:

NET.3.2.M1: Tulemüüride turvajuhend – hankija koostab oma üldise turvapoliitika alusel tulemüüride turvajuhendi, mis on kooskõlas organisatsiooni vajaduste ja standarditega. Teenuseandja järgib juhendit, hankija kontrollib juhendi järgmist.
NET.3.2.M2: Tulemüürireeglid – hankija vastutab oma turvapoliitikale ja vajadustele vastavate tulemüürireeglite kehtestamise eest, teenuseandja rakendab ja haldab reegleid.
NET.3.2.M3: Sobivad filtreerimisreeglid paketifiltris – hankija määratleb filtreerimisreeglid, mida teenuseandja rakendab ja haldab.
NET.3.2.M4: Tulemüüri turvaline konfigureerimine – teenuseandja vastutab tulemüüri konfigureerimise eest, hankija omab kontrolli konfiguratsiooni vastamise eest organisatsiooni turvanõuetele.
NET.3.2.M14: Tulemüüri käidudokumentatsioon – hankija on teadlik ja nõustub teenuseandja koostatud turvalisust mõjutavate toimingutega, mille lisab oma käidudokumentatsiooniga.

SYS.1.1: Server üldiselt[11] – serverites (nii füüsilistes kui virtuaalsetes) töödeldavate andmete ning nendega seotud serveriteenuste kaitse meetmed, täitmise eest vastutab IT-talitus

Hankija kohustused:

SYS.1.1.M1: Serverile juurdepääsu piiramine – hankija vastutab oma serverite füüsilise asukoha turvalisuse eest, piirates juurdepääsu ainult volitatud isikutele, teenuseandjale on volitatud isikute nimed edastatud.
SYS.1.1.M9: Kahjurvaratõrje rakenduste kasutamine serveril – hankija otsustab kahjurvaratõrje rakendamise vajalikkuse.
SYS.1.1.M11: Serveri turvajuhendi kehtestamine – hankija vastutab organisatsiooni turvapoliitikast ja vajadusest lähtuva serverite turvajuhendi koostamise ja rakendamise eest.
SYS.1.1.M12: Serveri kasutuselevõtu kava – hankija hindab riistvara parameetrite sobivust ja valikuid, nagu sooritusvõime, mälumaht ja läbilaskevõime, et server vastaks organisatsiooni vajadustele. Hankija veendub, et kõik turva- ja haldusmeetmed on paigas ja vastavad organisatsiooni turvanõuetele, otsused on vaja dokumenteerida.

[11] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/sys-itsuesteemid/sys1-server/sys11-server-ueldiselt/3-meetmed

SYS.1.1.M13: Serveri hankimine – hankija koostab nõuete spetsifikatsiooni ja infoturbe nõuded.
SYS.1.1.M22: Integreerimine avariivalmendusega – hankija koostab talituspidevuse kontseptsiooni koos andmevarunduse kavaga ning kehtestab taastekava ja harjutab seda regulaarselt.
SYS.1.1.M24: Regulaarne turbe testimine – hankija korraldab välisliideseid omavate serverite turvalisuse testimise ning kontrollib sisevõrgu serverite vastavust turvapoliitikatele, dokumenteerides tulemused.
SYS.1.1.M25: Serveri kasutuselt kõrvaldamise kord – hankija informeerib serveri kasutajaid selle kõrvaldamisest aegsasti, koostab serveri kõrvaldamiseks toimingute kontroll-loendi, koostab ülevaade serveril olevatest andmetest ja plaanitud uutest asukohtadest. Hankija tellib vajadusel enne serveri kasutuselt kõrvaldamist oluliste andmete varundamise.
SYS.1.1.M35: Serveri käidudokumentatsiooni haldus – hankija koostab ja uuendab regulaarselt iga tüüpserveri kohta käidudokumentatsiooni, sisaldab infoturbe vajadusi ning õigusaktidest tulenevaid nõudeid.

Teenuseandja kohustused:

SYS.1.1.M5: Haldusliideste kaitse – teenuseandja vastutab haldusliideste kaitsmise eest, tagades, et serveri välisseadmeid ja andmekandjaid kasutatakse ainult hoolduseks ning buutimine muudest seadmetest on desaktiveeritud. Teenuseandja desaktiveerib kõik tarbetud liidesed serveris.
SYS.1.1.M6: Tarbetute teenuste desaktiveerimine – teenuseandja desaktiveerib kõik tarbetud teenused ja funktsionaalsused serveris ning dokumenteerib serveri tarkvara, teenuste ja kontode konfiguratsioonid. Lisaks piirab teenuseandja kasutajale ja rakendustele antavat salvestusruumi ning desaktiveerib tarbetud serverikomponentide püsivara funktsioonid.
SYS.1.1.M15: Katkestusteta ja stabiilne toide – teenuseandja vastutab selle eest, et kõik serverid oleksid ühendatud piisava võimsuse ja aku kestvusega puhvertoiteallikaga.
SYS.1.1.M19: Lokaalsed paketifiltrid – teenuseandja kohustus on kaitsta suure kaitsetarbega servereid lokaalse paketifiltriga.
SYS.1.1.M21: Serveri käidudokumentatsiooni koostamine – teenuseandja peab koostama serveri käidudokumentatsiooni, milles on dokumenteeritud serveri käitusega seotud toimingud, konfiguratsioonimuudatused ja turvalisust puudutavad toimingud.
SYS.1.1.M23: Serverisüsteemi seire – teenuseandja vastutab serverisüsteemide seire eest, jälgides pidevalt serverisüsteemide olekut ja teenuste toimimist ning teavitades tõrgete korral serveri haldureid.
SYS.1.1.M34: Kõvaketta krüpteerimine – teenuseandja krüpteerib serveri andmekandjad usaldusväärsete vahenditega ning tagab, et krüptovõtmed ja -paroolid oleksid piisavalt tugevad ja kaitstud.
SYS.1.1.M36: Serveri buutimise turve – teenuseandja tagab serveri buutimise turvalisuse.
SYS.1.1.M37: Turvakriitiliste rakenduste ja operatsioonisüsteemi komponentide kapseldamine – teenuseandja vastutab turvakriitiliste rakenduste ja operatsioonisüsteemi komponentide kapseldamise eest ning tagab, et rakendusi, mis töötlevad ebaturvalistest allikatest pärit andmeid käitatakse operatsioonisüsteemist lahutatud täitmiskeskkonnas.
SYS.1.1.M39: Serveri turvaseadete keskne haldus – teenuseandja vastutab serveri turvaseadete keskse halduse eest, talletades serveri konfiguratsiooni keskses haldussüsteemis ja tagades, et serveri turvaseaded vastavad kehtestatud poliitikatele ja juhenditele.

Ühised kohustused:

SYS.1.1.M2: Kasutajate autentimine – hankija määratleb nõuded serverisse autentimiseks, teenuseandja vastutab nõuete rakendamise ja jõustamise eest majutatud süsteemides.
SYS.1.1.M10: Teenuseandja kehtestab ja dokumenteerib, milliseid sündmusi serveris logitakse ning kes ja millistel tingimustel võib logiandmeid vaadata. Hankija peab otsustama, kas

logiandmeid hoitakse serveris või kasutatakse keskset logiserverit ning teenuseandja tagan, et logitakse kõik turbe jaoks olulised sündmused.
SYS.1.1.M16: Serveri turvaline installimine ja aluskonfiguratsioon – hankija vastutab süsteemi- ja rakendustarkvara hankimise eest autentsetest ja usaldusväärsetest allikatest, tagades tarkvara legaalsuse ja turvalisuse; koostab turvajuhendid ja määrab kindlaks organisatsiooni vajadustele vastavad turvanõuded, millele serveri aluskonfiguratsioon peab vastama, hankija kontrollib turvaseade enne serveri käikuandmist ja pärast iga muudatust, tagamaks, et konfiguratsioon vastab turvanõuetele. Teenuseandja installib ja teeb esialgsed seadistused järgides tootja soovitusi ja organisatsiooni turvanõudeid ning tagab, et installitakse ainult serveri otstarbe täitmiseks vajalikud teenused.

SYS.1.2: Windows Server – kui PostgreSQLi andmebaaside majutus ja haldus toimub Windows Serveri platvormil, on need turvameetmed olulised. Kui kasutusel on mõni muu operatsioonisüsteem (nagu Linux), siis Windowsi spetsiifilised meetmed ei ole hanke suhtes otseselt asjakohased.

SYS.1.3: Linuxi ja Unixi server[12] – meetmed Linuxi operatsioonisüsteeme kasutavate serverite ja neis töödeldavate andmete käideldavuse, tervikluse ja konfidentsiaalsuse tagamiseks, meetmete täitmise eest vastutab IT-talitus
Hankija kohustused:
SYS.1.3.M2: Korrektne identifikaatorite määramine – hankija tagab, et kasutajanimed, UID-d ja GID-d on unikaalsed ning neid hallatakse süsteemselt kõigi organisatsiooni serverite ulatuses. Nõue on osa hankija sisekorralduses, rakendades organisatsioonisiseseid standardeid ja protseduure.
SYS.1.3.M4: Rakenduste kaitsmine – hankija vastutab rakenduste kaitse eest, kasutades ASLR-i ja DEP/NX-i, et tõsta turvanõrkuste ärakasutamise keerukust. See on seotud turvalisuse tagamisega hankija enda rakendustes.
Teenuseandja kohustused:
SYS.1.3.M3: Irdmäluseadmete automaatse failisüsteemiga sidumise vältimine – teenuseandja vastutab irdmäluseadmete automaatse failisüsteemiga sidumise vältimise eest.
SYS.1.3.M5: Tarkvarapakettide turvaline installimine – teenuseandja vastutab tarkvarapakettide turvalise installimise eest, hoolitsedes selle eest, et enne installimist kontrollitakse tarkvarapakettide terviklust ja autentsust.
SYS.1.3.M8: SSH-ga krüpteeritud andmevahetus – teenuseandja tagab SSH-ga krüpteeritud andmevahetuse, eelistades turvalist SSH protokolli ja desaktiveerides ebaturvalised andmevahetusprotokollid.
SYS.1.3.M10: Volitamata õiguste laiendamise takistamine – teenuseandja takistab volitamata õiguste laiendamise.
Ühised kohustused:
SYS.1.3.M6: Kasutajate ja rühmade haldus – hankija määratleb halduspoliitika ja nõuded, teenuseandja võib pakkuda vajalikke haldusvahendeid ja tehnilist tuge.

SYS.1.5: Virtualiseerimissüsteem[13] – meetmed virtualiseerimiskeskkonna ja virtuaalserverite turbe tagamiseks, meetmeid täidab IT-talitus
Hanke nõuded keskenduvad spetsiifiliselt PostgreSQL andmebaaside haldamisele ja majutamisele, hõlmates andmebaasi administratiivseid ülesandeid ja ressursside haldust. Kuigi

[12] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/sys-itsuesteemid/sys1-server/sys13-linuxi-ja-unixi-server
[13] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/sys-itsuesteemid/sys1-server/sys15-virtualiseerimissuesteem

virtualiseerimine võib olla osa teenuseandja pakutavast infrastruktuurist, ei ole see hanke nõuetes spetsiifiliselt välja toodud. Seetõttu võib järeldada, et need nõuded ei ole hanke põhifookuses või kriitilise tähtsusega.

Hankija kohustused:

SYS.1.5.M8: Virtualiseerimissüsteemi kavandamine – hankija vastutab virtualiseerimissüsteemi üldise arhitektuuri ja kavandamise eest tagamaks süsteemi sobivus organisatsiooni IT-poliitikatega.

SYS.1.5.M9: Virtualiseerimissüsteemi võrguarhitektuuri kavandamine – hankija vastutab virtualiseerimissüsteemi võrguarhitektuuri kavandamise eest, arvestades organisatsiooni IT-süsteemide, rakenduste ja võrkude nõudeid.

SYS.1.5.M10: Virtualiseerimissüsteemi halduse eeskiri – hankija kehtestab ja dokumenteerib virtuaalserverite ja virtualiseeritud IT-süsteemide haldamise eeskirjad.

Teenuseandja kohustused:

SYS.1.5.M2: Virtualiseerimissüsteemi turvaline rakendamine – teenuseandja vastutab virtualiseerimissüsteemi turvalise rakendamise eest.

SYS.1.5.M5: Virtualiseerimiskeskkonna haldusliideste turve – teenuseandja vastutab virtualiseerimiskeskkonna haldusliideste turvalisuse eest. See hõlmab haldusjuurdepääsu piiramist, haldusliideste eraldamist ebausaldusväärsetest võrkudest ning turvaliste protokollide kasutamist haldamiseks ja seireks.

SYS.1.5.M6: Virtualiseerimissüsteemi logimine – teenuseandja vastutab virtualiseerimissüsteemi logimise eest, logides süsteemi olekut ja võrguühendusi pidevalt.

SYS.1.5.M7: Aja sünkroonimine virtualiseerimissüsteemis – teenuseandja vastutab kellade sünkroonimise eest.

SYS.1.5.M11: Virtualiseerimissüsteemi haldusvõrk – teenuseandja vastutab virtualiseerimissüsteemi haldusvõrgu turvalisuse eest, kasutades eraldi haldusvõrku ning aktiveerides krüpteerimise turvamehhanismid.

SYS.1.5.M15: Erineva kaitsetarbega külalissüsteemide lahusus – teenuseandja vastutab erineva kaitsetasemega külalissüsteemide lahususe eest.

SYS.1.5.M16: Virtuaalmasinate isoleerimine – teenuseandja vastutab virtuaalmasinate isoleerimise eest.

SYS.1.5.M17: Virtualiseerimisserveri konfiguratsiooni kontrollimine ja seire – teenuseandja vastutab virtualiseerimisserveri konfiguratsiooni kontrollimise ja seire eest.

Ühised kohustused:

SYS.1.5.M3: Virtualiseerimiskeskkonna turvaline konfiguratsioon – nii hankija kui ka teenuseandja vastutavad virtualiseerimiskeskkonna turvalise konfiguratsiooni eest, sealhulgas külalissüsteemidele kehtestatavate piirangute eest. Teenuseandja rakendatav virtuaalsete külalissüsteemide ja nendes asuvate IT-süsteemide konfiguratsioon ja turve vastab organisatsiooni turvapoliitikale.

SYS.1.5.M4: Virtualiseerimistaristu turvaline võrgukonfiguratsioon – nii hankija kui ka teenuseandja vastutavad virtuaalserverite turvalise võrgukonfiguratsiooni eest, sealhulgas turvamehhanismide ja jälgimissüsteemide rakendamise eest.

SYS.1.5.M12: Virtualiseerimistaristu halduse õigused ja rollid – hankija ja teenuseandja kehtestavad halduse õigused ja rollid virtualiseerimistaristule.

SYS.1.5.M13: Virtualiseerimissüsteemi jaoks sobiv riistvara – hankija ja teenuseandja peavad tagama, et kasutatav riistvara ja selle tootetugi vastavad virtualiseerimislahenduse nõuetele.

SYS.1.5.M14: Virtualiseerimistaristu ühtsed konfiguratsiooninõuded – nii hankija kui ka teenuseandja vastutavad ühtsete konfiguratsiooninõuete määramise ja järgimise eest.

SYS.1.5.M19: Virtualiseerimissüsteemi regulaarsed läbivaatused – hankija kontrollib regulaarselt, kas virtualiseerimissüsteemi seisund vastab kavandatule, teenuseandja kontrollib, kas virtuaalsete komponentide konfiguratsioon vastab ettenähtud tüüpkonfiguratsioonile.

SYS.1.6: Konteinerdus[14] – meetmed konteinerites asuvate või konteineritega töödeldavate andmete kaitseks, meetmete rakendamise eest vastutab IT-talitus

Dokumentatsioonis ei ole konteinerduse ja sellele vastavate tehniliste nõuete kohta otseselt tingimusi, välja arvatud mittefunktsionaalsed nõuded SYS.1.6 seeria meetmete näol. Arvestades hanke spetsiifikat, ei tundu SYS.1.6 seeria meetmed (konteinerduse kavandamine, haldamine, turvaline käitamine, konteineritõmmiste kasutamine jne) otseselt relevantsetena, kuna need pole hanke nõuetes eraldi välja toodud. Seetõttu võib eeldada, et need meetmed ei pruugi need meetmed olla selle konkreetse hanke kontekstis olulised.

Hankija kohustused:

SYS.1.6.M1: Konteinerduse kavandamine – hankija vastutab konteinerduse eesmärkide ja ootuste määratlemise, riskide ja kulude hindamise eest.

SYS.1.6.M4: Konteineritõmmiste turvaline evitus – hankija vastutab turvaliste tõmmiste loomise ja rakendamise protsessi kavandamise ja dokumenteerimise eest.

SYS.1.6.M9: Rakenduste sobivuse hindamine – hankija on testinud konteineris kasutatavate rakenduste ja teenuste sobivus.

SYS.1.6.M10: Konteinerite kasutamise eeskiri – hankija koostab konteinerite käitamise reeglid.

SYS.1.6.M15: Konteineri ressursipiirangute määratlemine – hankija määrab konteineri hostsüsteemi ressursid ning koostab tegevuskava juhuks, kui ressurssidele määratud piirväärtused ületatakse.

Teenuseandja kohustused:

SYS.1.6.M5: Konteinerite haldusvõrgu eraldamine – teenuseandja eraldab konteinerite haldusvõrgu, mis tagab piisava turvataseme, piirates hostsüsteemi haldusvõrku, konteinerite haldusvõrku ja konteinerdatud rakendustele juurdepääsuks kasutatavaid võrke üksteisest asjakohaselt ning blokeerides mittevajalikud andmesideühendused.

SYS.1.6.M6: Turvaliste konteineritõmmiste kasutamine – teenuseandja vastutab turvaliste konteineritõmmiste kasutamise eest, tagab, et kõik kasutatavad konteineritõmmised pärinevad usaldusväärsetest allikatest, enne kasutuselevõttu on konteineri sisu kontrollitud turvanõrkuste suhtes.

SYS.1.6.M7: Konteineri logiandmete säilitamine – teenuseandja vastutab konteineri logiandmete säilitamise eest, tagab, et logiandmed salvestatakse ja säilitatakse väljaspool konteinerit vähemalt hostsüsteemi tasemel.

SYS.1.6.M8: Konteineri pääsuandmete turvaline haldus – teenuseandja vastutab konteineri pääsuandmete turvalise halduse eest, rakendades mandaatide ja juurdepääsuandmete salvestamisel ning haldamisel turvamehhanisme.

SYS.1.6.M11: Rakenduste eraldamine konteinerites – teenuseandja eraldab rakendused konteinerites, tagades, et iga konteiner kannab samaaegselt ainult üht IT-teenust.

SYS.1.6.M13: Konteineritõmmiste kasutuseks kinnitamine – teenuseandja kinnitab konteineritõmmised kasutuseks, tagades, et konteineritõmmised testitakse enne käituskeskkonda paigaldamist, nende kasutamine kinnitatakse vastavalt kehtestatud korrale.

SYS.1.6.M14: Konteineritõmmiste ajakohastamine – teenuseandja vastutab konteineritõmmiste ajakohastamise eest, uuendite paigaldamine toimub kinnitatud muudatusehalduse protsessi kohaselt ning otsustades pikaajaliselt kasutuses olnud konteinerite uuendamise vajaduse üle.

SYS.1.6.M16: Konteinerite kaughoolduse turve – teenuseandja vastutab konteinerite kaughoolduse turve eest, tagades, et kõiki konteineritest hostide suunas ja vastupidi tehtavaid

[14] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/sys-itsuesteemid/sys1-server/sys16-konteinerdus

haldustegevusi käsitletakse kaughooldusena ning piirates kaughooldusjuurdepääse konteinerite käituskeskkonda.
SYS.1.6.M17: Konteineri käitamiseks minimaalselt vajalike õiguste määratlemime – teenuseandja vastutab konteineri käitamiseks minimaalselt vajalike õiguste määratlemise eest, tagades, et konteineri käituskeskkonda ja selles loodud konteinereid käitatakse selleks otstarbeks loodud lihtkasutaja õigustega kontodega ning täiendavad meetmed võetakse kasutusele konteineri käituskeskkonna kapseldamiseks.
SYS.1.6.M18: Konteinerdatud rakenduste õiguste piiramine – teenuseandja vastutab konteinerdatud rakenduste õiguste piiramise eest, tagab, et konteinerisisestel süsteemikontodel ei ole õigusi hostsüsteemis, vajalikud juurdepääsuõigused antakse ainult konteinerile salvestisüsteemist.
SYS.1.6.M19: Andmesalvestitele juurdepääsu reguleerimine – teenuseandja vastutab andmesalvestitele juurdepääsu reguleerimise eest, tagab, et konteineritel on juurdepääs ainult tööks vajalikele andmesalvestitele ning juurdepääs on antud määral, mis on tööülesannete täitmiseks vajalik.
SYS.1.6.M20: Konteineri konfiguratsiooniandmete turve – teenuseandja vastutab konteineri konfiguratsiooniandmete turve eest, konfiguratsiooniandmed on versioonitud ning kõik konfiguratsioonimuudatused on dokumenteeritud.
Ühised kohustused:
SYS.1.6.M2: Konteinerduse halduse kavandamine – hankija ja teenuseandja (turvauuenduste paikamine) on kaasatud konteinerduse elutsükli ja turvahalduse kavandamisse.
SYS.1.6.M3: Konteinerdatud IT-süsteemide turvaline käitamine – mõlemad osapooled tagavad, et konteinerdus ei kahjusta olemasolevate süsteemide turvalisust ja töökindlust (teenuseandja – Konteinerite käitamisel seiratakse süsteemi toimivust ning viiakse läbi perioodilisi seisundikontrolle).
SYS.1.6.M12: Konteineritõmmiste turvaline levitamine – hankija tagab, et koostatud kriteeriumid, mille alusel hinnatakse konteinertõmmiste usaldusäärsust, teenuseandja tagab vajalikud metaandmed ja kaitstuse volitamata muutmise eest.

SYS.1.8: Salvestilahendused
SYS.1.8 meetmed on üldistatud meetmed andmete salvestamise ja säilitamise turvalisuse tagamiseks. Need meetmed hõlmavad salvestisüsteemide füüsilist paigaldust, turvalist aluskonfiguratsiooni, haldusliideste turvele ja muid sarnaseid aspektide. Kuna need meetmed keskenduvad rohkem spetsiifiliselt salvestisüsteemide tehnilistele aspektidele, ei pruugi need olla otse seotud konkreetses hankes määratletud PostgreSQL andmebaaside haldamise ja majutamise nõuetega.

SYS.2.1: Klientarvuti üldiselt; SYS.2.1: Klientarvuti üldiselt; SYS.2.2: Windows kliendid; SYS.2.3: Linuxi ja Unixi klient; SYS.2.4: macOS-i klient
Kõnealune hange keskendub peamiselt PostgreSQL andmebaaside majutamisele ja haldusele, siiski on klientarvuti turvalisus ja haldus kriitilised aspektid igas IT infrastruktuuris, eriti andmebaaside haldamise ja juurdepääsu kontekstis. Klientarvutite turvaline autentimine, uuenduste haldamine, kahjurvaratõrje ja muud sarnased meetmed on hädavajalikud, et tagada, et hankija IT-keskkonna turvalisus ja vastupidavus erinevatele turvariskidele, mis võivad mõjutada andmebaaside tõhusust ja turvalisust.

Hanke raames võib tekkida vajadus andmebaasidele ligipääsuks ja halduseks klientarvutite kaudu. Autentimisprotseduurid, turvaline buutimine, uuenduste haldamine ja kahjurvaratõrje on standardprotseduurid, mis aitavad kaasa üldisele IT-süsteemi turvalisusele, olles samuti olulised andmebaaside majutamise ja haldamise kontekstis.

Kuigi klientarvutite turvalisus on oluline igas IT-süsteemis, ei pruugi see olla peamine fookus konkreetses hankes, mis keskendub rohkem serveripõhisele infrastruktuurile ja andmebaaside haldusele.

APP.4.3: Andmebaasisüsteemid[15] – meetmed relatsioonandmebaasisüsteemide turvaliseks kavandamiseks, rajamiseks ja käitamiseks ning andmebaasides töödeldava teabe kaitseks, meetmete täitmise eest vastutab IT-talitus

Hankija kohustused:

APP.4.3.M4: Uute andmebaaside kasutuselevõtu reguleerimine – hankija määrab protseduuri uute andmebaaside kasutuselevõtuks.

APP.4.3.M11: Riistvara dimensioneerimine – hankija jälgib, et ressursid vastaksid organisatsiooni vajadustele, isegi kui teenuseandja teostab dimensioneerimise.

APP.4.3.M17: Andmete laadimise ja migratsiooni korraldus – hankija kehtestab protseduurid.

APP.4.3.M19: Mittekvaliteetsete skriptide vältimine – hankija määrab skriptide kvaliteedistandardid.

APP.4.3.M20: Regulaarne läbivaatus – hankija vastutab süsteemi regulaarse läbivaatamise eest.

Teenuseandja kohustused:

APP.4.3.M9: Andmebaasisüsteemi varundamine – teenuseandja vastutab andmebaasisüsteemi varundamise eest, see hõlmab regulaarset varundamist, sealhulgas enne andmebaasi loomist, ning taastamisparameetrite määramist vastavalt andmete kaitsetarbele. Teenuseandja kaalub varunduse kontseptsiooni muutmist juhul, kui ette nähtud mahtusid ületatakse.

APP.4.3.M13: Lingitud andmebaaside piirangud – teenuseandja vastutab andmebaasi linkide piirangute tagamise eest, annab õigusi linkide loomiseks ainult määratud isikutele, teostab linkide dokumenteerimist ja regulaarset kontrollimist.

APP.4.3.M16: Andmebaasiühenduste krüpteerimine – teenuseandja vastutab andmebaasiühenduste krüpteerimise eest, tagab, et kõik andmebaasiühendused on krüpteeritud vastavalt kaitsetarbele ning vastavad krüpteerimisprotseduurid ja mehhanismid.

Ühised kohustused:

APP.4.3.M1: Andmebaasisüsteemi turvaeeskiri – hankija vastutab turvaeeskirja koostamise eest, teenuseandja vastutab eeskirja järgmise eest.

APP.4.3.M3: Andmebaasihalduse süsteemi turvalisuse tõstmine – teenuseandja koostab tugevdamise meetmetest kontroll-loendi, hankija kontrollib rakendamist.

APP.4.3.M12: Andmebaasihalduse süsteemi tüüpkonfiguratsioon – tüüpkonfiguratsiooni koostamine on hankija vastutada, järgimine on teenuseandja ülesanne. Kontrollib hankija.

APP.4.3.M18: Andmebaasisüsteemi seire – süsteemi seire on teenuseandja kohustus, hankija tagab, et see vastab tema vajadustele.

CON.2: Isikuandmete kaitse[16] - meetmed rakendatakse äriprotsesside kaitseks tagamaks andmeid töötleva organisatsiooni turvalisus, isikuandmete kaitse meetmete rakendamise eest vastutab organisatsiooni juhtkond

Hankija kohustused:

CON.2.M1: Isikuandmete kaitse kavandamine – hankija vastutab töödeldavate isikuandmete asukohtade, liikide ja kaitsetarbe analüüsi ning seadusandlusest ja kolmandate osapooltega sõlmitud lepingutest tulenevate andmekaitsenõuete kaardistamise ja dokumenteerimise eest.

---

[15] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/app-rakendused/app4-aerirakendused/app43-andmebaasisuesteemid/3-meetmed

[16] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/con-kontseptsioonid-ja-metoodikad/con2-isikuandmete-kaitse/3-meetmed

CON.2.M2: Andmekaitsespetsialisti määramine – hankija määrab organisatsiooni andmekaitsespetsialisti ja hoiab tema teadmised ajakohasena.
CON.2.M3: Isikuandmete töötluse kaardistamine – hankija vastutab isikuandmete töötlemise kaardistamise ja dokumenteerimise eest.
CON.2.M4: Andmekaitsepoliitika ja andmekaitsejuhiste väljatöötamine – hankija töötab välja ja rakendab andmekaitsepoliitika ja -juhised.
CON.2.M5: Organisatsiooni töötajate teadlikkuse tõstmine – hankija korraldab organisatsiooni andmekaitsealaseid koolitusi.
CON.2.M6: Isikuandmete töötlemise õigus- ja eesmärgipärasuse ning minimaalsuse tagamine – hankija vastutab isikuandmete töötluse õiguspärasuse tagamise eest.
CON.2.M7: Andmekaitsetingimuste dokumenteerimine – hankija koostab andmekaitsetingimused.
CON.2.M9: Isikuandmete pseudonüümimine ja anonüümimine – hankija vastutab isikuandmete pseudonüümimise ja anonüümimise eest.
CON.2.M10: Isikuandmetele juurdepääsu piiramine – hankija määratleb juurdepääsuõigused.
CON.2.M11: Isikuandmete korrakohane säilitamine – hankija määrab säilitustähtajad ja -eesmärgid.
CON.2.M12: Isikuandmete kaitse tehniliste meetmete rakendamine – hankija koostab andmekaitsetingimused ja rakendab tehnilised meetmed.
CON.2.M13: Andmekaitsealased mõjuhinnangud – hankija viib läbi andmekaitsealase mõjuhinnangu ja koostab mõjuhinnangu läbiviimise juhendi.
CON.2.M16: Isikuandmete säilitamise eeskiri – hankija koostab isikuandmete säilitamise eeskirja.
CON.2.M17: Keskne pääsuhalduse süsteem – hankija kasutab ja haldab keskset pääsuhalduste süsteemi.
CON.2.M22: Lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtete rakendamine rakendustes – hankija tagab, et rakendused järgivad andmekaitse põhimõtteid.
CON.2.M23: Isikuandmeid sisaldavate rakenduste testimine – hankija koostab põhimõtted rakenduste testide läbiviimiseks ning sõlmib testimise läbiviimise lepingud ning teostab testimisjärgse järelkontrolli.
CON.2.M24: Privaatsusseadistused veebilehtedel – hankija rakendab oma kodulehel isikuandme kaitseks turvaameetmeid, annab külastajatele teave jälgmisvahendite kohta.
CON.2.M25: Isikuandmete kustutamine töötaja lahkumisel – hankija koostab eeskirjad.
CON.2.M26: Andmekaitseauditi läbiviimine – hankija viib läbi regulaarseid andmekaitseauditeid.

Teenuseandja kohustused:

CON.2.M20: Andmetöötluse asukohtade füüsiline turvalisus – teenuseandja, olles hankija andmete füüsiline hoidja, tagab isikuandmete füüsilise turvalisuse: määrab piiratud pääsuga alad ja kehtestab juurdepääsureeglid. See hõlmab tehniliste juurdepääsu- ja valvesüsteemide rakendamist. Teenuseandja töötab välja protseduurid külaliste haldamiseks, et tagada isikuandmete töötlemise aladele kontrollitud ja turvaline juurdepääs.
CON.2.M21: Võrguturbe tagamine – teenuseandja tagab, et isikuandmete saatmiseks avaliku võrgu kaudu kasutatakse turvalisi ja krüpteeritud protokolle.

Ühised kohustused:

CON.2.M8: Andmesubjekti õiguste tagamine – nii hankija kui teenuseandja tagavad, et andmesubjektide õigusi saab IT-süsteemides tehniliselt rakendada.
CON.2.M14: Volitatud töötlejate haldus – mõlemad osapooled tagavad, et volitatud töötlejad järgivad turvameetmeid.
CON.2.M15: Isikuandmete turvaline krüpteerimine – krüpteerimise tagamine on ühine vastutus.

CON.2.M18: Isikuandmete töötlemise turve – hankija määratleb turvanõuded ja -poliitikad, teenuseandja rakendab ja haldab neid.
CON.2.M19: Andmetöötluse toimingute logimine – hankija kehtestab logimise põhimõtted, teenuseandja haldab ja analüüsib logisid.

CON.3: Andmevarunduse kontseptsioon[17] - juhised organisatsiooni andmevarunduse kontseptsiooni koostamiseks ja rakendamiseks andmete kaitseks, meetmete täitmise eest vastutab infoturbejuht
Hankija kohustused:
CON.3.M1: Andmevarunduse mõjurite piiritlemine – hankija koostab varundatavate andmete registri ja määrab andmevarunduse mõjurid.
CON.3.M2: Andmevarunduseeskiri – hankija koostab andmevarunduseeskirja.
CON.3.M4: Andmevarundusplaanid – hankija koostab andmevarundusplaani, kaasa arvatud varunduse ja andmetaaste põhimõtted.
CON.3.M6: Andmevarunduse kontseptsioon – hankija koostab andmevarunduse kontseptsiooni ning kooskõlastab selle vastutajatega ning kontrollib rakendamist.
CON.3.M7: Sobiva andmevarundussüsteemi soetamine – hankija valib ja soetab sobiva andmevarundussüsteemi.
CON.3.M9: Tingimuste tagamine kaugvarunduseks – hankija tagab teenusetasemelepingu sõlmimise ja määrab tingimusted tagamaks kaugvarunduse efektiivse ja turvalise toimimise.
CON.3.M15: Varunduse regulaarne testimine – hankija testib regulaarselt andmevarunduse toimimist ja varundatud andmete taastamist.
Teenuseandja kohustused:
CON.3.M12: Varunduseks kasutatavate andmekandjate turvaline säilitus – teenuseandja säilitab varunduseks kasutatavate andmekandjate turvaliselt hoides andmekandjaid lähtesüsteemist eraldi. Teenuseandja peab tagama andmete turvalise säilituse vähemalt nõutud andmesäilitustähtaegade ulatuses.
Ühised kohustused:
CON.3.M5 Regulaarne andmevarundus – hankija määrab andmevarunduse regulaarsuse ja korralduse, teenuseandja järgib kehtestatud ajakava ja protseduure.
CON.3.M14: Varukoopiate turve – hankija määrab turvastandardid ja -nõuded, teavitab töötajaid korraldusest, teenuseandja järgib standardeid ja nõudeid.

ORP.4: Identiteedi- ja õiguste haldus[18] - meetmed identiteedi- ja õiguste halduse korraldamiseks, meetmete täitmise eest vastutab IT-talitus
Hankija kohustused:
ORP.4.M1: Kasutajakontode halduse eeskiri – hankija koostab ja kinnitab kasutajakontode halduse eeskirja, kuna see nõuab organisatsioonisiseste poliitikate ja protseduuride määratlemist.
ORP.4.M4: Kohustuste jaotamine ja kohustuste lahusus – hankija määrab kohustused ja tööülesanded, sealhulgas infotehnoloogia kasutamise nõuded, meede hõlmab organisatsiooni sisemiste protseduuride ja tööjaotuse määratlemist.
ORP.4.M5: Füüsilise ligipääsu haldamine – hankija vastutab füüsilise ligipääsu õiguste määramise ja haldamise eest hankija vastutusalas.

[17] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/con-kontseptsioonid-ja-metoodikad/con3-andmevarunduse-kontseptsioon/3-meetmed
[18] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/orp-organisatsioon-ja-personal/orp4-identiteedi-ja-ooiguste-haldus/3-meetmed

ORP.4.M7: Andmetele juurdepääsu haldamine – hankija määrab vajalikud andmete juurdepääsuõigused, juhendab andmepääsuõigusega isikuid juurdepääsuvahendeid õigesti kasutama.
ORP.4.M11: Paroolide lähtestamine ja muutmine – hankija kehtestab paroolide lähtestamiseks või muutmiseks piisavalt turvalised protseduurid.
ORP.4.M17: Sobiv identiteedi- ja õiguste halduse süsteem – hankija valib ja kohandab identiteedi- ja õiguste halduse süsteemi valiku ja kohaldamisala oma vastutusalas, eeldab süsteemi sobitamist organisatsiooni äriprotsesside ja kaitsetarvetega.
ORP.4.M18: Keskse autentimisteenuse kasutamine – hankija kavandab ja dokumenteerib keskse autentimisteenuse turvanõuded.
ORP.4.M19: Töötajate juhendamine autentimisprotseduuride ja -mehhanismide kasutamisel – hankija tutvustab organisatsiooni töötajatele autentimise korda ning juhendab kasutama, koostab töötajatele autentimisjuhised.
ORP.4.M22: Parooli kvaliteedinõuete kehtestamine – hankija määrab paroolinõuded.

Teenuseandja vastutada:

ORP.4.M10: Eeliskontode kaitsmine – teenuseandja kaitseb eeliskontosid, rakendades mitmikautentimist väliste ründajate ja õiguste volitamata laiendamise vastu.
ORP.4.M14: Kasutajakontode kasutuse kontrollimine – teenuseandja kontrollib kasutajakontode kasutamist, tagades, et kasutajad kasutavad oma kontot regulaarselt ja logivad pärast ülesande täitmist süsteemist alati välja.
ORP.4.M16: IT-süsteemidele juurdepääsu reguleerimine – teenuseandja vastutab IT-süsteemidele juurdepääsu reguleerimise eest, järgib kehtestatud pääsupoliitikaid ja kasutab standardseid õiguste profiile vastavalt töötaja ülesannetele.
ORP.4.M23: Nõuded paroole töötlevatele IT-süsteemidele – teenuseandja vastutab paroole töötlevate IT-süsteemide turvalisuse eest, paroole ei talletata avateksti kujul ning võrgustatud IT-süsteemide ja rakenduste paroole edastatakse alati krüpteeritult. Teenuseandja tagab, et paroolide vahetamine toimub alati konkreetsel põhjusel ning et süsteemides kasutatavad vaikimisi paroolid ja sisselogimissätted muudetakse esimesel võimalusel piisavalt tugevateks.

Ühised kohustused:

ORP.4.M2: Õiguste andmine, muutmine ja tühistamine – hankija määrab protseduurid, teenuseandja rakendab ja haldab neid, tagades pääsuõiguste andmise ja tühistamise vastavalt vajadusele.
ORP.4.M3: Kasutajate õiguste dokumenteerimine – hankija koostab dokumentatsiooni ja selle ajakohasuse, teenuseandja tagab, et õigused ja turvalisuse.
ORP.4.M6: IT-vahenditele juurdepääsu haldamine – hankija määrab juurdepääsuõigused, teenuseandja haldab neid ja tagab korrektse IT-vahendite juurdepääsu reguleerimise.
ORP.4.M8: Paroolide kasutamise kord – hankija kehtestab paroolide kasutamise korra, teenuseandja tagab korra rakendamise ja järgimise.
ORP.4.M9: Tuvastamine ja autentimine – hankija määrab autentimisnõuded, teenuseandja rakendab nõudeid, tagamaks turvalise tuvastamise ja autentimise.
ORP.4.M12: IT-süsteemide ja rakenduste autentimiskord – hankija määrab iga IT-süsteemi ja rakenduse jaoks autentimisnõuded ja kehtestab autentimiskorra. Teenuseandja rakendab nõudeid.
ORP.4.M13: Sobivate autentimismehhanismide valimine – hankija määra organisatsiooni kaitsetarbele vastavad tuvastus- ja autentimismehhanisid. Teenuseandja rakendab need.
ORP.4.M15: Identiteedi- ja õiguste halduse protseduurid – hankija koostab protseduurid pääsupoliitikate haldamiseks, kasutajakontode ja kasutajarühmade haldamiseks, õiguste profiilide ja kasutajarollide haldamiseks. Teenuseandja rakendab protseduurid.

OPS.1.1.2: IT-haldus[19] - meetmed IT-süsteemide ja võrkude turvaliseks halduseks, meetmete täitmise eest vastutab IT-talitus

Hankija kohustused:

OPS.1.1.2.M4: IT-haldurina töötamise lõpetamine – hankija tagab, et IT-halduri lahkumisel blokeeritakse kõik seotud kontod ja eemaldatakse pääsuõigused. Samuti vastutab hankija uute kontaktisikute määramise eest kolmandate pooltega suhtlemisel.

OPS.1.1.2.M7: IT-halduri kohustuste määramine – hankija määrab IT-halduri kohustused ja tagab tööülesannete selge jaotuse.

OPS.1.1.2.M23: IT-süsteemide halduse rollide ja kasutajaõiguste määramise põhimõtted – hankija kehtestab põhimõtted, tagamaks juurdepääsuõiguste ja rollide läbipaistva organisatsiooni vajadusele vastamise.

OPS.1.1.2.M24:IT-süsteemide haldustoimingute kontrollimine – hankija kontrollib kehtestatud põhimõtete järgimist.

Teenuseandja kohustused:

OPS.1.1.2.M5: Halduskonto tegevuste kontrollimine – teenuseandja tagab, et igal IT-halduril ja tema asendajal on personaalne eeliskonto, mida kasutatakse üksnes haldustoiminguteks ning kõik haldustoimingud on tagantjärele tuvastatavad.

OPS.1.1.2.M8: Rakenduste haldus – teenuseandja vastutab rakenduste halduse eest, mis hõlmab rakenduste- ja süsteemihaldurite vaheliste ülesannete jaotuse määratlemist ning dokumenteerimist ning rakenduse kasutajatega kooskõlastamist enne IT-halduri sekkumist rakenduse käitamisse. Teenuseandja tagab, et halduse käigus tehtud muudatused on korrektselt dokumenteeritud ja neile on juurdepääs ka IT-halduri eemaloleku korral.

OPS.1.1.2.M16: Halduspääsu tehniline eraldamine – teenuseandja vastutab halduspääsu tehnilise eraldamise eest, milleks kasutatakse tehnilisi meetmeid nagu eraldatud võrgusegmendid ja hüppeserverid, mis tagavad, et haldusliidestele on juurdepääs vaid selleks volitatud isikutel ning need ei ole otse välisvõrguga ühendatud.

OPS.1.1.2.M25: IT-süsteemide halduse toimingute läbiviimise ajastamine – teenuseandja vastutab IT-halduse toimingute läbiviimise ajastamise eest, kõik haldustoimingud viiakse läbi eelnevalt kasutajaid teavitades või kavandatud hooldusakna jooksul.

OPS.1.1.2.M26: IT-komponentide konfiguratsiooni varundamine – teenuseandja vastutab IT-komponentide konfiguratsiooni varundamise eest, tagab, et kehtivast konfiguratsioonist on varukoopia enne haldustoimingute teostust ning et võimalike negatiivsete tagajärgedega toimingute puhul varundatakse konfiguratsioon täiendavalt enne toimingute alustamist.

Ühised kohustused:

OPS.1.1.2.M2: IT-haldurite asendamise kord – hankija määrab asendamise korra, teenuseandja tagab, et asendajad on kvalifitseeritud ja neil on vajalikud õigused.

OPS.1.1.2.M6: Halduskontode turve – hankija määrab autentimismehhanismid, teenuseandja vastutab nende rakendamise ja järgimise eest.

OPS.1.1.2.M21: IT-süsteemide halduse rollide määramine – hankija ja teenuseandja määravad mõlemad halduse rollid, tagades nende vastavuse IT-süsteemide vajadustele ja minimaalsuse põhimõttele.

OPS.1.1.2.M28: IT-süsteemide haldustoimingute logimine– hankija määrab logimise nõuded, teenuseandja vastutab, et logimine nõuetekohase toimimise ja logide terviklikkuse tagamise.

[19] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops1-oma-kaeidutoeoed/ops11-itpoohitoeoed/ops112-ithaldus/3-meetmed

OPS.1.1.3: Paiga- ja muudatusehaldus[20] - meetmed organisatsiooni paiga- ja muudatusehalduse protseduuride kohaldamiseks, juhtimiseks ja optimeerimiseks, meetmete täitmise eest vastutab IT-talitus

Hankija kohustused:

OPS.1.1.3.M6: Muudatuste kooskõlastamine – hankija loob muudatuste kooskõlastamise protsessi.

OPS.1.1.3.M10: Tarkvaratoodete tervikluse ja autentsuse tagamine – hankija hangib tarkvara ja selle uuendused usaldusväärsetest allikatest ning kontrollib nende autentsust.

OPS.1.1.3.M11: Infotöötluse pidev dokumenteerimine – hankija tagab organisatsiooni IT-süsteemide muudatuste pideva dokumenteerimise, muudatused on korrektselt registreeritud ja jälgitavad.

Teenuseandja kohustused:

OPS.1.1.3.M9: Uue riistvara testimise ja kasutuselevõtu protseduurid – teenuseandja vastutab uue riistvara testimise ja kasutuselevõtu protseduuride eest, tagab, et enne uue riistvara kasutuselevõttu testitakse seda põhjalikult spetsiaalselt selleks loodud testkeskkonnas, mis on eraldatud käidukeskkonnast.

Ühised kohustused:

OPS.1.1.3.M1: Paiga- ja muudatusehalduse kord – hankija kehtestab paiga- ja muudatusehalduse korra. Mõlemad osapooled vastutavad paikade ja uuenduste testimise ja tagasivõtmise protseduuride eest.

OPS.1.1.3.M2: Vastutuse määramine – hankija määrab vastutajad paiga- ja muudatusehalduse eest, teenuseandja aktsepteerib ja korraldab muudatuste läbiviimise.

OPS.1.1.3.M3: Automaatuuenduste turvaline seadistus – hankija määratleb uuendusmehhanismide kontrolli ja konfiguratsiooni nõuded, teenuseandja tagab vastavalt juhisele uuenduste turvalise rakendamise ja haldamise.

OPS.1.1.3.M5: Muutmistaotluste käsitlus – hankija vastutab muutmistaotluste protsessi kehtestamise eest, teenuseandja tagab muudatuste tehnilise elluviimise.

OPS.1.1.3.M7: Muudatusehalduse sobitamine äriprotsessidega – hankija tagab muudatusehalduse kooskõla äriprotsessidega, teenuseandja viib muudatused ellu tagades nende integreerimise organisatsiooni tegevustesse.

OPS.1.1.3.M8: Paiga- ja muudatusehalduse tööriistade turvaline rakendamine – hankija kehtestab turvanõuded ja valib tööriistad, teenuseandja tagab nende turvalise rakendamise ja haldamise.

OPS.1.1.3.M15: IT-süsteemide regulaarne uuendamine – hankija määrab uuendamise poliitika, teenuseandja tagab uuenduste korrektse paigalduse, mõlemad osapooled kontrollivad uuenduste rakendamise korrektsust.

OPS.1.1.5: Logimine[21] - meetmed logiandmete turvaliseks kogumiseks, talletamiseks, analüüsimiseks ja nõuetekohaseks kõrvaldamiseks, täitmise eest vastutab IT-talitus

Hankija kohustused:

OPS.1.1.5.M1: Logimise eeskiri – hankija kehtestab logimise eeskirja. See hõlmab logimise planeerimist, korraldamist ja rakendamist, mis peavad olema kooskõlas infoturvapoliitikaga. Hankija kontrollib täitmist.

Teenuseandja kohustused:

OPS.1.1.5.M3: Sündmuste logimise konfigureerimine – teenuseandja konfigureerib sündmuste logimise. Teenuseandja peab tagama, et logimise eeskirjaga hõlmatud IT-süsteemides ja

[20] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops1-oma-kaeidutoeoed/ops11-itpoohitoeoed/ops113-paiga-ja-muudatusehaldus/3-meetmed

[21] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops1-oma-kaeidutoeoed/ops11-itpoohitoeoed/ops115-logimine/3-meetmed

rakendustes on kasutusele võetud sisemised logimisfunktsioonid ning nende toimimist ja korrektsust kontrollitakse regulaarselt.
OPS.1.1.5.M4: Aja sünkroniseerimine – teenuseandja tagab kellade sünkroonimise logitavate IT-süsteemide ja rakenduste vahel, et logid oleksid ajaliselt täpsed.
OPS.1.1.5.M8: Logiandmete arhiveerimine – teenuseandja arhiveerib logiandmed vastavalt logimise eeskirjale ja asjakohastele õigusaktidele.
Ühised kohustused:
OPS.1.1.5.M5: Õiguslike raamtingimuste täitmine – hankija tagab logimisprotsesside andmekaitse ja muude asjakohaste õigusaktide järgimise nõudeid, teenuseandja rakendab protseduure.
OPS.1.1.5.M6: Keskse logitaristu rajamine – hankija loob keskse logitaristu strateegia eest, teenuseandjakuid rakendab ja haldab seda.
OPS.1.1.5.M9: Logiandmete valmendus analüüsimiseks – hankija määrab logiandmete arhiveerimise ja analüüsimise protseduurid, teenuseandja viib neid läbi.
OPS.1.1.5.M10: Logiandmete kaitse lubamatu juurdepääsu eest – hankija määrab logiandmete kaitse põhimõtted, teenuseandja rakendab ja haldab neid, sealhulgas tõkestab volitamata juurdepääsu.

OPS.1.1.6: Tarkvara testimine ja kasutuselevõtt[22] - tarkvara testimise ja kasutuselevõtu soovituslikud protseduurid ning meetmed kasutusele võetava tarkvara tehnilistele ja korralduslikele turvanõuetele vastavuse tagamiseks, täitmise eest vastutab IT-talitus
Hanke kirjelduses ei ole spetsiifiliselt käsitletud tarkvara testimise temaatikat. Hanke kirjelduses keskendutakse peamiselt PostgreSQL andmebaasisüsteemide majutamise teenusele, sealhulgas nende halduse, majutamise, ressursihalduse ja muude seonduvate teenuste pakkumisele. Kuigi tarkvara testimine võib moodustada osa laiemast IT-infrastruktuuri haldamise või tarkvaraarenduse protsessist, ei ole see aspekt konkreetselt esile tõstetud.
Hankija kohustused:
OPS.1.1.6.M1: Tarkvara testimise kavandamine – hankija määrab testimise raamtingimused, mis on kooskõlas kaitsetarbe ja tehniliste võimalustega, sealhulgas tagab testimiskeskkonna sarnasuse käidukeskkonnaga.
OPS.1.1.6.M4: Tarkvara kinnitamine – hankija kinnitav struktuuriüksus kontrollib tarkvara nõuetekohase testimise ja kinnitab selle kasutuselevõtu.
OPS.1.1.6.M6: Tarkvara testija juhendamine – hankija teavitab tarkvara testijat piisava ajavaruga ning tutvustab tarkvara kasutusviise ja täiendavaid nõudeid.
OPS.1.1.6.M10: Testimise vastuvõtu kord – hankija kehtestab testimise vastuvõtu korra, määratledes kohustuslikud testid, oodatavad tulemused ja testimise vastuvõtu kriteeriumid.
Teenuseandja kohustused:
OPS.1.1.6.M2: Tarkvara funktsionaaltestimine – teenuseandja vastutab tarkvara funktsionaaltestimise eest, kõiki tarkvara funktsioone kontrollitakse tarkvara funktsionaaltestimise käigus, veendumaks nende nõuetekohases toimimises.
OPS.1.1.6.M3: Testimistulemuste analüüsimine – teenuseandja analüüsib testimistulemusi, testitulemuste analüüsi käigus võrreldakse testimisel saadud tegelikke väärtusi oodatavate tulemustega ning dokumenteeritakse analüüsi tulemused.
OPS.1.1.6.M11: Testandmete anonüümimine või pseudonüümimine – teenuseandja vastutab testandmete anonüümimise või pseudonüümimise eest, et kaitsmaks tundlikke andmeid.

[22] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops1-oma-kaeidutoeoed/ops11-itpoohitoeoed/ops116-tarkvara-testimine-ja-kasutuselevoott/3-meetmed

OPS.1.1.6.M7: Personali valimine tarkvara testijaks – teenuseandja valib personaali tarkvara testijateks, tagab, et testijatel on vajalik erialane kvalifikatsioon ning teadmised kasutatavatest programmeerimiskeeltest, arenduskeskkondadest ja testimismeetoditest.
OPS.1.1.6.M13: Testkeskkonna lahutamine käidukeskkonnast – teenuseandja lahutab testkeskkonna käidukeskkonnast, et tagada tarkvara testimine vaid selleks ettenähtud keskkonnas ning vältida testimisest tulenevaid riske või häireid käidukeskkonnas.
OPS.1.1.6.M15: Paigaldamise ja seadistamise juhendi järgimine – teenuseandja valmistab ette tarkvara testkeskkonna vastavalt tarkvara paigaldamise ja seadistamise juhendile.

Ühised kohustused:

OPS.1.1.6.M5: Mittefunktsionaalsete testide tegemine – hankija ja teenuseandja teevad koostööd tarkvara jõudluse, kvaliteedinäitajate ja turvalisuse testimisel, kus teenuseandja viib läbi testid hankija määratletud ulatuses ja nõuetes.
OPS.1.1.6.M12: Regressioontestimine – hankija määratleb testimise nõuded ja protseduurid, teenuseandja viib läbi testimise.

OPS.1.1.7: Süsteemihaldus[23] - meetmed süsteemihalduse lahenduse, selle komponentide ja hallatavate IT-süsteemide turvaliseks konfigureerimiseks, seireks ja andmevahetuseks, täitmise eest vastutab IT-talitus

Hankija kohustused:

OPS.1.1.7.M1: Süsteemihalduse nõuete määratlemine – hankija määratleb süsteemihalduse nõuded, sealhulgas turvanõuded.
OPS.1.1.7.M8: Süsteemihalduse kontseptsioon – hankija koostab süsteemihalduse kontseptsiooni, mis hõlmab meetodeid, tehnikaid ja turvalisust.
OPS.1.1.7.M9: Süsteemihalduse rakendusplaan – hankija koostab süsteemihalduse rakendusplaani, mis on kooskõlas organisatsiooni turvaeeskirjaga.
OPS.1.1.7.M16: Süsteemihalduse integreerimine avariivalmendusega – hankija on integreerinud süsteemihalduse lahenduse organisatsiooni avariivalmenduse kontseptsiooniga. ning lisanud andmete taaste taasteplaanidesse.

Teenuseandja kohustused:

OPS.1.1.7.M3: Kellade sünkroniseerimine – teenuseandja sünkroniseerib kellad.
OPS.1.1.7.M11: Süsteemihalduse regulaarne lahknevusanalüüs – teenuseandja vastutab süsteemihalduse regulaarse lahknevusanalüüsi eest, mis hõlmab andmete tervikluse kontrollimist, süsteemide konfiguratsioonide vastavust keskselt kavandatud konfiguratsioonidele ning skriptide ja muude automaatsete tegevuste õigsuse kontrollimist.
OPS.1.1.7.M12: Keskne süsteemihalduse toimingute käivitamine – teenuseandja tagab keskse süsteemihalduse toimingute käivitamise, et hallatavates IT-süsteemides saaks süsteemihalduse toiminguid käivitada ainult süsteemihalduse lahendus ning aktiveeritud oleksid ainult vajalikud haldusfunktsioonid.
OPS.1.1.7.M13: Lubatud haldusliideste määramine – teenuseandja määrab lubatud haldusliidesed, tagab, et haldusjuurdepääs hallatavatele süsteemidele oleks lubatud ainult määratud süsteemihalduse lahenduse liideste kaudu ning dokumenteerib erandjuhtude kasutamist ja tehtud muudatusi.
OPS.1.1.7.M14: Keskne hallatavate IT-süsteemide konfiguratsioonihaldus – teenuseandja vastutab keskse hallatavate IT-süsteemide konfiguratsioonihalduse eest, tagab konfiguratsioonide täieliku ja ajakohase halduse, juurdepääsu ainult volitatud tarbijatele ning süsteemihalduse lahenduse ja hallatavate IT-süsteemide vahelise andmevahetuse turvalisuse.

[23] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops1-oma-kaeidutoeoed/ops11-itpoohitoeoed/ops117-suesteemihaldus/3-meetmed

OPS.1.1.7.M17: Süsteemihalduse andmevahetuse piiramine – teenuseandja piirab süsteemihalduse andmevahetust, kasutades sobivaid tööriistu andmevahetuse piiramiseks minimaalselt vajalikule määrale.
OPS.1.1.7.M18: Süsteemihalduse lahenduse seisundi kontroll – teenuseandja kontrollib süsteemihalduse lahenduse seisundit.
OPS.1.1.7.M19: Süsteemihalduse lahenduse andmeside turve – teenuseandja vastutab süsteemihalduse lahenduse andmeside turbe eest, tagab süsteemihalduse lahenduse ja hallatavate süsteemide vahelise krüpteeritud andmeside.
Ühised kohustused:
OPS.1.1.7.M2: Süsteemihalduse lahenduse kavandamine – hankija määratleb nõuded, teenuseandja kavandab süsteemihalduse nõuetele vastava lahenduse.
OPS.1.1.7.M4: Süsteemihalduse andmeside kaitse – hankija määratleb nõuded, teenuseandja rakendab neid, tagamaks andmeside turvalisuse.
OPS.1.1.7.M5: Vastastikune autentimine – hankija kehtestab autentimise nõuded, teenuseandja rakendab neid.
OPS.1.1.7.M6: Juurdepääsu turve – hankija kehtestab juurdepääsu turvalisuse nõuded, teenuseandja rakendab ja haldab neid.
OPS.1.1.7.M7: Süsteemihalduse turvaeeskiri – hankija koostab ja kontrollib regulaarselt süsteemihalduse turvaeeskirja, teenuseandja järgib eeskirja.
OPS.1.1.7.M10: Süsteemihalduse turvalise käituse juhised – hankija koostab juhise, mis arvestab kehtestatud turvanõudeid, teenuseandja järgib juhiseid.
OPS.1.1.7.M15: Süsteemihalduse lahenduse seire, logimine ja teavitused – hankija määratleb olulised sündmused, teenuseandja teostab logimise.

OPS.2.1: Väljasttellimine[24] (numbrid valed) – meetmed väljasttellimise turvaeesmärkide saavutamiseks ja infoturbe parendamiseks kogu allhanke elutsükli kestel, täitmise eest vastutab IT-talitus
Hankija kohustused:
OPS.2.3.M1: Turvanõuded väljasttellitavale teenusele – hankija määratleb väljasttellitavate teenuste turvanõuded, mis põhinevad organisatsiooni kaitsetarbe määramisel ja ärimõjude hindamisel.
OPS.2.3.M2 Riskipõhine lähenemine hangete korraldamisel – hankija hindab riskipõhiselt teenuse väljasttellimise võimalikkust.
OPS.2.3.M3: Teenuseandja valimise kriteeriumid – hankija määratleb teenuseandja valimise kriteeriumid, valideerima valitud teenuseandja vastavuse kriteeriumidele ning kontrollima pidevalt vastavust.
OPS.2.3.M7: Välisteenuselepingu korrakohane lõpetamine – hankija lepib kokku teenuselepingu lõpetamise tingimustes ja protseduurides.
OPS.2.3.M8: Väljasttellimise strateegia koostamine – hankija koostab organisatsiooni majanduslikke, tehnilisi, korralduslikke ja õiguslikke raamtingimusi ning infoturbe aspekte käsitlev väljasttellimise strateegia.
OPS.2.3.M9: Hankepoliitika kehtestamine – hankija kehtestab väljasttellimise hankepoliitika.
OPS.2.3.M11 Väljasttellitud teenuste register – hankija koostab ja haldab väljasttellitud teenuste registrit.
OPS.2.3.M12 Väljasttellitud teenuste aruandlus – hankija vastutab teenuste aruandluse eest.

[24] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops2-kaeidutoeoed-teenusena/ops21-vaeljasttellimine/3-meetmed

OPS.2.3.M13: Huvide konflikti vältimine teenuselepingu sõlmimisel – teenuselepingu tingimuste läbirääkimisel osalevad hankija organisatsiooni erinevate valdkondade esindajad, vältides võimalikku äripoole ja infoturbe huvide konflikti.
OPS.2.3.M14 Laiendatud nõuded teenuselepingule -– hankija määrab teenuselepingus millistele objektidele ja võrguteenustele tohib teenuseandja hankija võrgus juurde pääseda, dokumenteerib peamised sooritusindikaatorid.
OPS.2.3.M16 Teenuseandja infoturbe läbivaatus – hankija kontrollib teenuseandja infoturbe rakendamist.
OPS.2.3.M18: Teenuseandjaga sõlmitud lepete läbivaatus – hankija hindab lepetes sisalduvate meetmete asja- ja ajakohasust ning täiendab vajadusel lepet.
OPS.2.3.M19: Alternatiivsete teenuseandjate kaardistamine – hankija koostab tegevuskavad teenuse erakorraliseks lõpetamiseks ning on kaardistanud potentsiaalsed teenuseandjad.

Teenuseandja kohustused:

OPS.2.3.M5: Teenuseandja simultaanteeninduse võimekuse hindamine – teenuseandja vastutab simultaanteeninduse võimekuse hindamise eest, see hõlmab kliendi andmete turvalist eraldamist erinevate klientide teenuste pakkumisel ja nõuab tehnilise kirjelduse esitamist andmekaitse meetmete kohta.
OPS.2.3.M17: Teenuseandja personali kasutamise kord – teenuseandja vastutab personali kasutamise korra eest, see nõuab teenuseandja töötajatele kliendi juures kehtivate nõuete selgitamist ja nende järgimise kinnitamist ning kokkulepet töötajate asendamise ja töösuhte lõpetamise protseduuride osas.

Ühised kohustused:

OPS.2.3.M4: Teenuselepingu vastavus kliendi nõuetele – hankija tagab, et teenuseleping katab kõik vajalikud aspektid, kaasa arvatud turvanõuded ja lepingupartnerite õigused ja kohustused. Teenuseandja tagab nõuete täitmise kontrollimiseks vajalikud teabe saamise ja juurdepääsu õigused ning vajadusel ka auditeerimisvõimalused.
OPS.2.3.M6 Väljasttellitava teenuse turbe põhimõtted – teenuseandja rakendab hankija määratletud turvameetmeid, hankija kontrollib meetmete piisavust ja vastavust nõuetele.
OPS.2.3.M10: Vastutavate kontaktisikute määramine – hankija ja teenuseandja määravad oma organisatsioonisisesed suhtluspartnerid.
OPS.2.3.M15: Teenuseandja ja kliendi turvaline võrguühendus – mõlemad pooled lepivad kokku ja dokumenteerivad võrguühenduse tingimused.
OPS.2.3.M20 Avariivalmendus väljasttellimisel – hankija koostab avariivalmenduse plaani, teenuseandja tagab, et nende süsteemid ja protseduurid on sellega kooskõlas.

OPS.2.2: Pilvteenuste kasutamine[25] – meetmed pilvteenuste turvaliseks kasutuselevõtuks ja kasutamiseks, meetmete täitmise eest vastutab IT-talitus

Hankija kohustused:

OPS.2.2.M1: Pilvteenuste strateegia – hankija kehtestab organisatsiooni eesmärkidega kooskõlas olleva pilvteenuste strateegia. Hankija viib läbi ka teostatavuse, tasuvuse ja turvalisuse analüüsi igale kavandatavale pilvteenusele.
OPS.2.2.M2: Pilvteenuste turvapoliitika – hankija koostab pilvteenuste turvapoliitika, lähtudes teenuse kaitsetarbest ja korralduslikest, tehnilistest ning õiguslikest raamtingimustest.
OPS.2.2.M3 Pilvteenuste loendi koostamine – hankija dokumenteerib kõik kavandatavad ja kasutatavad pilvteenused.
OPS.2.2.M4: Vastutusalade ja liidestuste määramine – hankija määratleb ja dokumenteerib pilvteenuse kasutamisega seotud vastutusalad ja tegevused.

[25] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops2-kaeidutoeoed-teenusena/ops22-pilvteenuste-kasutamine/3-meetmed

OPS.2.2.M5 Pilvteenusele migreerimise kava – hankija koostab asjakohaseid tegevusi ja protseduure hõlmava pilvteenusele migreerimise kava.
OPS.2.2.M6: Pilvteenusega liitumise tegevusplaan - hankija koostab pilvteenuse kasutuselevõtuks tegevusplaani, mis hõlmab ka liidestuste ettevalmistust ja võrguühenduste kontrollimist. Hankija uuendab tegevusplaani.
OPS.2.2.M7: Pilvteenuste turbe programm – hankija koostab pilvespetsiifilisi riske arvestava turbe programmi.
OPS.2.2.M8: Pilvteenuse andja valimise kriteeriumid – hankija koostab nõuete spetsifikatsiooni.
OPS.2.2.M9: Kliendi vajadustele vastav pilvteenuse leping – hankija kinnitab, et pilvteenuse leping on vastavuses organisatsiooni vajaduste ja turvanõuetega.
OPS.2.2.M11: Pilvteenuse avariivalmenduse programm – hankija töötab välja kõiki asjakohaseid aspekte ja protseduure katva pilvteenuste avariivalmenduse programmi.
OPS.2.2.M14: Pilvteenuselepingu korrakohane lõpetamine – hankija kehtestab protseduurid pilvteenuselepingu lõpetamiseks.

Teenuseandja kohustused:

OPS.2.2.M10: Turvaline migratsioon pilvteenusele – teenuseandja arvestab eelnevalt väljatöötatud kava ja turbe programmi, testib migratsiooni toimimist testkeskkonnas ning kontrollib teenuse vastavust lepingu tingimustele pärast IT-süsteemide migreerimist käidukeskkonda.

Ühised kohustused:

OPS.2.2.M12: Infoturve pilvteenuste kasutamisel – hankija kontrollib pilvteenuse tingimusi ja turvanõudeid. Teenuseandja järgib intoturbe teadlikkuse suurendamise ning IT-süsteemide halduse meetmeid. Avariikäsitlust harjutatakse ühiselt.
OPS.2.2.M13: Pilvteenuste turbe piisavuse tõendamine – pilvteenuse andja tõendab infoturbele vastavust, hankija veendub, pilvteenuse andja turvemeetmete vastavuses õigusaktidele ja rahvusvahelistele standarditele.

OPS.3.1: Teenuseandja infoturve[26] – meetmed teenuseandja infoturbe kavandamiseks, rakendamiseks, juhtimiseks ja kontrollimiseks ning nõutava turbetaseme hoidmiseks teenuseandja vaatest, täitmise eest vastutab IT-talitus

Hankija kohustused:

OPS.3.2.M9: Teenuselepingute perioodiline läbivaatus – hankija vastutab lepingutes sätestatud turvameetmete jätkuva asjakohasuse kontrollimise eest.

Teenuseandja kohustused:

OPS.3.2.M1: Teenuseosutamise põhimõtted – teenuseandja vastutab teenuste turbe kavandamise eest, see hõlmab klientide infoturbe vajaduste arvestamist teenuste kavandamisel ning võimekust tagada klientidele minimaalselt lubatav infoturbe tase vastavalt seadusandlusest tulenevatele nõuetele.
OPS.3.2.M2: Teenuse tarneleping kliendiga – teenuseandja koostab tüüptingimustega teenuselepingu.
OPS.3.2.M3: Väljasttellitava teenuse turbe programm – teenuseandja vastutab turvanõuete tagamise eest allhankijate kasutamisel.
OPS.3.2.M4: Klientide andmete eraldamise põhimõtted – teenuseandja vastutab klientide andmete eraldamise põhimõtete eest.
OPS.3.2.M5: Teenuseandja personali kasutamise kord – teenuseandja koostab turvakontseptsiooni, see hõlmab kõigi pakutavate teenuste turvameetmete üldist kavandamist

[26] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops3-teenuseandja-kaeidutoeoed/ops31-teenuseandja-infoturve/3-meetmed

ja klientidega kooskõlastamist, tagades seeläbi klientidele turvalise teenuse ning võimaluse muuta vajadusel turvakontseptsiooni vastavalt klientide erisoovidele.
OPS.3.2.M6: Teenuseandja välispersonali kasutamise kord – teenuseandja töötab välja teenuselepingu korralise ja erakorralise lõpetamise korra.
OPS.3.2.M7: Simultaanteeninduse kord – teenuseandja koostab allhankijate asendamise korra.
OPS.3.2.M8: Kliendi võrgu kasutamise kokkulepe – teenuseandja vastutab teenuse osutamise põhimõtete dokumenteerimise eest.
OPS.3.2.M12: Muudatuste haldus – teenuseandja vastutab protsesside ja IT-süsteemide riskianalüüsi eest, see nõuab riskide hindamist enne uute rakenduste, IT-süsteemide või protsesside klientidele kättesaadavaks tegemist.
OPS.3.2.M13: Turvaline migratsioon välisteenusele – teenuseandja loob turvalised andmesidekanalid.
OPS.3.2.M14: Välisteenuse avariivalmendus – teenuseandja vastutab protsesside ja IT-süsteemide pideva seire eest.
OPS.3.2.M16: Teenuse tarneahela läbipaistvuse tagamine – teenuseandja tagab teenuse tarneahela läbipaistvuse.
OPS.3.2.M17: Pääsu reguleerimine – teenuseandja vastutab pääsu reguleerimise eest, see nõuab sobivate korralduslike ja tehniliste vahendite kasutamist teenuseandja ja kliendi töötajate sissepääsu ja juurdepääsu reguleerimiseks.
OPS.3.2.M18: Allhankija töötajate teadlikkuse tõstmine – teenuseandja vastutab allhankija töötajate teadlikkuse tõstmise eest, see eeldab allhankija töötajate koolitamist ja informeerimist nende tööülesannete täitmisest ning kehtivatest infoturbe nõuetest ja konfidentsiaalsuslepingutest kinnipidamise kinnitamist.

Ühised kohustused:

OPS.3.2.M10: Turvaliste suhtluskanalite loomine ja kontaktisikute määramine – mõlemad osapooled peavad kokku leppima suhtluskanalites ja kontaktisikutes ning kontrollima nende volituste kehtivust.
OPS.3.2.M11: Teenuste avariivalmenduse plaan – mõlemad osapooled vastutavad omavahelise avariivalmenduse plaani kooskõlastamise eest.
OPS.3.2.M15: Klientidele esitatavad aruanded – hankija ja teenuseandja lepivad kokku, tüüparuanded ning kasutatavad suhtluskanalid.

Lisa 2 – Riigihanke „Infosüsteemide majutusteenuse tellimine ETIS ja EHIS" detailne analüüs

Antud lisa toob detailse analüüsi, kuidas meetmed jagunevad detailselt hankija, teenuseandja ning teenuseandja ja hankija vahel. Kuna hange on koostatud ISKE meetmeid silmas pidades, on eraldi välja toodud, milliseid E-ITSi meetmeid ei ole ISKEs olemas ja millised neist on erineva meetmeklassiga.

Hankedokument kirjeldab teenust, mis käsitleb EHISe ja ETISe keskkondade majutust ja administreerimisteenust kirjeldades hetkeolukorda ning hõlmates hankija süsteemide füüsilist kolimist teenuseandja majutuskeskkonda. Hankija infosüsteemide majutamiseks vajalik taristu ja selle haldamine sisaldab järgmisi alaosasid: serverite ja teiste süsteemide majutamiseks vajaliku taristu pakkumine, infosüsteemide majutusteenus serveriruumis, internetiühenduse teenus, tulemüüriteenus, mis eraldab infosüsteemide sisevõrgu välisest võrkudest, serverite ja muu taristu riistvara ning tarkvara (nii süsteemse kui ka rakendustarkvara) haldamisteenus.

Iga teenuse osa käsitleb konkreetseid ülesandeid ja nõudeid, tagamaks infosüsteemide tõhusat ja turvalist majutamist ning haldamist. Teenuse osutamisel tuleb arvestada ISKE M turbetaseme nõuetega, tagades infosüsteemide ja nendega seotud andmete ja tarkvara turvalisuse.

ISKE pakub kolme turbeastet: madalat (L), keskmist (M) ja kõrget (H), infovarade turbeastme määramise järgselt tuleb leida igale infovarale vastavad tüüpmoodulid. Tüüpmoodulite spetsifikatsioonides on ka loetelu rakendamisele kuuluvatest turvameetmetest.

Hankija soovitud teenuse – EHISe ja ETISe keskkondade majutus ja administreerimisteenusega on otseselt seotud järgmised E-ITSi moodulid:

- Hoone ja ruumi (INF): oluline andmekeskuste ja serveriruumide puhul, kus keskkondi majutatakse. See tagab füüsilise turvalisuse;
- ORP.4 Identiteedi- ja õiguste haldus: infosüsteemide majutamise ja administreerimise teenuse puhul on oluline tagada, et õigused ja identiteedid on õigesti hallatud, eriti seoses serverite ning süsteemide haldamise ja kasutajatoega;
- OPS.1.1.2 IT-süsteemide haldus: teenus hõlmab serverite ja muu taristu majutamist ning haldamist, on IT-süsteemide korrektne haldus oluline;
- OPS.1.1.3 Paiga- ja muudatusehaldus: tagamaks infosüsteemide nõuetekohane töö, on vajalik efektiivne paiga- ja muudatusehaldus;
- OPS.1.1.4 Kaitse kahjurprogrammide eest: turvalisuse tagamiseks on vajalik süsteemide kaitse kahjurprogrammide ja pahavara eest;
- OPS.1.1.5 Logimine: süsteemide monitooring ja intsidentide haldus eeldab tegevuste logimist;
- OPS.1.1.6 Tarkvara testimine ja kasutuselevõtt: tagamaks uute rakenduste ja süsteemide turvaline kasutuselevõtt;
- DER.2.1 Turvaintsidentide käsitlus: võimalike turvaintsidentide efektiivne käsitlus on kriitilise tähtsusega teenuse osutamise käigus;
- NET.3.2 Tulemüür: eraldab infosüsteemide sisevõrku välisest võrkudest, on vajalik teenuse osa;
- CON.3 Andmevarunduse kontseptsioon: andmevarundus on oluline teenuse osa, et tagada andmete säilivus ja taastatavus.

Hoone ja ruumi (INF. Taristu)[27]:
E-ITSi turvameetmete rakendamise eest vastutab teenuseandja sellistes valdkondades nagu hoone üldine turvalisus, serveriruumid ja andmekeskused, tehnilise taristu ruumid, kaabeldus ning hoonete tehniline haldus. INF.12: Kaabeldus ja INF.13: Hoonete tehniline haldus, mille eest samuti vastutab teenuseandja, puuduvad ISKEst.

ORP.4: Identiteedi- ja õiguste haldus[28] – meetmed identiteedi- ja õiguste halduse korraldamiseks, meetmete täitmise eest vastutab IT-talitus
Hankija kohustused:
ORP.4.M1: Kasutajakontode halduse eeskiri – hankija koostab ja kinnitab kasutajakontode halduse eeskirja, kuna see nõuab organisatsioonisiseste poliitikate ja protseduuride määratlemist.
ORP.4.M4: Kohustuste jaotamine ja kohustuste lahusus – hankija määrab kohustused ja tööülesanded, sealhulgas infotehnoloogia kasutamise nõuded, meede hõlmab organisatsiooni sisemiste protseduuride ja tööjaotuse määratlemist.
ORP.4.M5: Füüsilise ligipääsu haldamine – hankija vastutab füüsilise ligipääsu õiguste määramise ja haldamise eest hankija vastutusalas.
ORP.4.M7: Andmetele juurdepääsu haldamine – hankija määrab vajalikud andmete juurdepääsuõigused, juhendab andmepääsuõigusega isikuid juurdepääsuvahendeid õigesti kasutama.
ORP.4.M11: Paroolide lähtestamine ja muutmine – hankija kehtestab paroolide lähtestamiseks või muutmiseks piisavalt turvalised protseduurid.
ORP.4.M17: Sobiv identiteedi- ja õiguste halduse süsteem – hankija valib ja kohandab identiteedi- ja õiguste halduse süsteemi valiku ja kohaldamisala oma vastutusalas, eeldab süsteemi sobitamist organisatsiooni äriprotsesside ja kaitsetarvetega.
ORP.4.M18: Keskse autentimisteenuse kasutamine – hankija kavandab ja dokumenteerib keskse autentimisteenuse turvanõuded.
ORP.4.M19: Töötajate juhendamine autentimisprotseduuride ja -mehhanismide kasutamisel – hankija tutvustab organisatsiooni töötajatele autentimise korda ning juhendab kasutama, koostab töötajatele autentimisjuhised.
ORP.4.M22: Parooli kvaliteedinõuete kehtestamine – hankija määrab paroolinõuded.
Teenuseandja kohustused:
ORP.4.M10: Eeliskontode kaitsmine – teenuseandja kaitseb eeliskontosid, rakendades mitmikautentimist väliste ründajate ja õiguste volitamata laiendamise vastu.
ORP.4.M14: Kasutajakontode kasutuse kontrollimine – teenuseandja kontrollib kasutajakontode kasutamist, tagades, et kasutajad kasutavad oma kontot regulaarselt ja logivad pärast ülesande täitmist süsteemist alati välja.
ORP.4.M16: IT-süsteemidele juurdepääsu reguleerimine – teenuseandja vastutab IT-süsteemidele juurdepääsu reguleerimise eest, järgib kehtestatud pääsupoliitikaid ja kasutab standardseid õiguste profiile vastavalt töötaja ülesannetele.
ORP.4.M23: Nõuded paroole töötlevatele IT-süsteemidele – teenuseandja vastutab paroole töötlevate IT-süsteemide turvalisuse eest, paroole ei talletata avateksti kujul ning võrgustatud IT-süsteemide ja rakenduste paroole edastatakse alati krüpteeritult. Teenuseandja tagab, et paroolide vahetamine toimub alati konkreetsel põhjusel ning et süsteemides kasutatavad vaikimisi paroolid ja sisselogimissätted muudetakse esimesel võimalusel piisavalt tugevateks.
Ühised kohustused:

[27] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/inf-taristu/inf1-hoone-ueldiselt/3-meetmed
[28] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/orp-organisatsioon-ja-personal/orp4-identiteedi-ja-ooiguste-haldus/3-meetmed

ORP.4.M2: Õiguste andmine, muutmine ja tühistamine – hankija määrab protseduurid, teenuseandja rakendab ja haldab neid, tagades pääsuõiguste andmise ja tühistamise vastavalt vajadusele.
ORP.4.M3: Kasutajate õiguste dokumenteerimine – hankija koostab dokumentatsiooni ja selle ajakohasuse, teenuseandja tagab, et õigused ja turvalisuse.
ORP.4.M6: IT-vahenditele juurdepääsu haldamine – hankija määrab juurdepääsuõigused, teenuseandja haldab neid ja tagab korrektse IT-vahendite juurdepääsu reguleerimise.
ORP.4.M8: Paroolide kasutamise kord – hankija kehtestab paroolide kasutamise korra, teenuseandja tagab korra rakendamise ja järgimise.
ORP.4.M9: Tuvastamine ja autentimine – hankija määrab autentimisnõuded, teenuseandja rakendab nõudeid, tagamaks turvalise tuvastamise ja autentimise.
ORP.4.M12: IT-süsteemide ja rakenduste autentimiskord – hankija määrab iga IT-süsteemi ja rakenduse jaoks autentimisnõuded ja kehtestab autentimiskorra. Teenuseandja rakendab nõudeid.
ORP.4.M13: Sobivate autentimismehhanismide valimine – hankija määra organisatsiooni kaitsetarbele vastavad tuvastus- ja autentimismehhanisid. Teenuseandja rakendab need.
ORP.4.M15: Identiteedi- ja õiguste halduse protseduurid – hankija koostab protseduurid pääsupoliitikate haldamiseks, kasutajakontode ja kasutajarühmade haldamiseks, õiguste profiilide ja kasutajarollide haldamiseks. Teenuseandja rakendab protseduurid.
ISKE sisaldab kõiki meetmeid.

OPS.1.1.2: IT-haldus[29] – meetmed IT-süsteemide ja võrkude turvaliseks halduseks, meetmete täitmise eest vastutab IT-talitus

Hankija kohustused:

OPS.1.1.2.M4: IT-haldurina töötamise lõpetamine – hankija tagab, et IT-halduri lahkumisel blokeeritakse kõik seotud kontod ja eemaldatakse pääsuõigused. Samuti vastutab hankija uute kontaktisikute määramise eest kolmandate pooltega suhtlemisel.
OPS.1.1.2.M7: IT-halduri kohustuste määramine – hankija määrab IT-halduri kohustused ja tagab tööülesannete selge jaotuse.
OPS.1.1.2.M23: IT-süsteemide halduse rollide ja kasutajaõiguste määramise põhimõtted – hankija kehtestab põhimõtted, tagamaks juurdepääsuõiguste ja rollide läbipaistva organisatsiooni vajadusele vastamise.
OPS.1.1.2.M24:IT-süsteemide haldustoimingute kontrollimine – hankija kontrollib kehtestatud põhimõtete järgimist.

Teenuseandja kohustused:

OPS.1.1.2.M5: Halduskonto tegevuste kontrollimine – teenuseandja tagab, et igal IT-halduril ja tema asendajal on personaalne eeliskonto, mida kasutatakse üksnes haldustoiminguteks ning kõik haldustoimingud on tagantjärele tuvastatavad.
OPS.1.1.2.M8: Rakenduste haldus – teenuseandja vastutab rakenduste halduse eest, mis hõlmab rakenduste- ja süsteemihaldurite vaheliste ülesannete jaotuse määratlemist ning dokumenteerimist ning rakenduse kasutajatega kooskõlastamist enne IT-halduri sekkumist rakenduse käitamisse. Teenuseandja tagab, et halduse käigus tehtud muudatused on korrektselt dokumenteeritud ja neile on juurdepääs ka IT-halduri eemaloleku korral.
OPS.1.1.2.M16: Halduspääsu tehniline eraldamine – teenuseandja vastutab halduspääsu tehnilise eraldamise eest, milleks kasutatakse tehnilisi meetmeid nagu eraldatud võrgusegmendid ja hüppeserverid, mis tagavad, et haldusliidestele on juurdepääs vaid selleks volitatud isikutel ning need ei ole otse välisvõrguga ühendatud.

[29] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops1-oma-kaeidutoeoed/ops11-itpoohitoeoed/ops112-ithaldus/3-meetmed

OPS.1.1.2.M25: IT-süsteemide halduse toimingute läbiviimise ajastamine – teenuseandja vastutab IT-halduse toimingute läbiviimise ajastamise eest, kõik haldustoimingud viiakse läbi eelnevalt kasutajaid teavitades või kavandatud hooldusakna jooksul.
OPS.1.1.2.M26: IT-komponentide konfiguratsiooni varundamine – teenuseandja vastutab IT-komponentide konfiguratsiooni varundamise eest, tagab, et kehtivast konfiguratsioonist on varukoopia enne haldustoimingute teostust ning et võimalike negatiivsete tagajärgedega toimingute puhul varundatakse konfiguratsioon täiendavalt enne toimingute alustamist.
Ühised kohustused:
OPS.1.1.2.M2: IT-haldurite asendamise kord – hankija määrab asendamise korra, teenuseandja tagadab, et asendajad on kvalifitseeritud ja neil on vajalikud õigused.
OPS.1.1.2.M6: Halduskontode turve – hankija määrab autentimismehhanismid, teenuseandja vastutab nende rakendamise ja järgimise eest.
OPS.1.1.2.M21: IT-süsteemide halduse rollide määramine – hankija ja teenuseandja määravad mõlemad halduse rollid, tagades nende vastavuse IT-süsteemide vajadustele ja minimaalsuse põhimõttele.
OPS.1.1.2.M28: IT-süsteemide haldustoimingute logimine – hankija määrab logimise nõuded, teenuseandja vastutab, et logimine nõuetekohase toimimise ja logide terviklikkuse tagamise.
ISKE ei kata järgnevaid meetmeid: kõik OPS.1.1.2.

OPS.1.1.3: Paiga- ja muudatusehaldus[30] – meetmed organisatsiooni paiga- ja muudatusehalduse protseduuride kohaldamiseks, juhtimiseks ja optimeerimiseks, meetmete täitmise eest vastutab IT-talitus
Hankija kohustused:
OPS.1.1.3.M6: Muudatuste kooskõlastamine – hankija loob muudatuste kooskõlastamise protsessi.
OPS.1.1.3.M10: Tarkvaratoodete tervikluse ja autentsuse tagamine – hankija hangib tarkvara ja selle uuendused usaldusväärsetest allikatest ning kontrollib nende autentsust.
OPS.1.1.3.M11: Infotöötluse pidev dokumenteerimine – hankija tagab organisatsiooni IT-süsteemide muudatuste pideva dokumenteerimise, muudatused on korrektselt registreeritud ja jälgitavad.
Teenuseandja kohustused:
OPS.1.1.3.M9: Uue riistvara testimise ja kasutuselevõtu protseduurid – teenuseandja vastutab uue riistvara testimise ja kasutuselevõtu protseduuride eest, tagab, et enne uue riistvara kasutuselevõttu testitakse seda põhjalikult spetsiaalselt selleks loodud testkeskkonnas, mis on eraldatud käidukeskkonnast.
Ühised kohustused:
OPS.1.1.3.M1: Paiga- ja muudatusehalduse kord – hankija kehtestab paiga- ja muudatusehalduse korra. Mõlemad osapooled vastutavad paikade ja uuenduste testimise ja tagasivõtmise protseduuride eest.
OPS.1.1.3.M2: Vastutuse määramine – hankija määrab vastutajad paiga- ja muudatusehalduse eest, teenuseandja aktsepteerib ja korraldab muudatuste läbiviimise.
OPS.1.1.3.M3: Automaatuuenduste turvaline seadistus – hankija määratleb uuendusmehhanismide kontrolli ja konfiguratsiooni nõuded, teenuseandja tagab vastavalt juhisele uuenduste turvalise rakendamise ja haldamise.
OPS.1.1.3.M5: Muutmistaotluste käsitlus – hankija vastutab muutmistaotluste protsessi kehtestamise eest, teenuseandja tagab muudatuste tehnilise elluviimise.

[30] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops1-oma-kaeidutoeoed/ops11-itpoohitoeoed/ops113-paiga-ja-muudatusehaldus/3-meetmed

OPS.1.1.3.M7: Muudatusehalduse sobitamine äriprotsessidega – hankija tagab muudatusehalduse kooskõla äriprotsessidega, teenuseandja viib muudatused ellu tagades nende integreerimise organisatsiooni tegevustesse.
OPS.1.1.3.M8: Paiga- ja muudatusehalduse tööriistade turvaline rakendamine – hankija kehtestab turvanõuded ja valib tööriistad, teenuseandja tagab nende turvalise rakendamise ja haldamise.
OPS.1.1.3.M15: IT-süsteemide regulaarne uuendamine – hankija määrab uuendamise poliitika, teenuseandja tagab uuenduste korrektse paigalduse, mõlemad osapooled kontrollivad uuenduste rakendamise korrektsust.
ISKEs on kirjeldatud kõik OPS 1.1.3. OPS 1.1.6. Sealhulgas ISKE meetmed L ja M on E-ITSis kõrgmeetmete hulgas, OPS.1.1.5.M11, OPS.1.1.5.M12, OPS.1.1.5.M12, OPS.1.1.5.M13.

OPS.1.1.4: Kaitse kahjurprogrammide eest[31] – meetmed kahjurprogrammide vastase kaitse korraldamiseks, täitmise eest vastutab IT-talitus
Hankija kohustused:
OPS.1.1.4.M1: Kahjurprogrammide tõrje kontseptsioon – hankija koostab kontseptsiooni, milliseid IT-süsteeme kahjurprogrammide eest kaitstakse ja kuidas ning väldib IT-süsteemide kasutamist, kuni neid on võimalik kahjurvara eest usaldatavalt kaitsta. Hankija hoiab kahjurtõrje programmi relevantsena.
OPS.1.1.4.M2: Süsteemikohaste turvamehhanismide kasutamine – hankija on dokumenteerinud, millised turvamehhanismid on kasutatavatesse IT-süsteemidesse lisatud.
OPS.1.1.4.M7: Kasutajate teadlikkuse suurendamine – hankija korraldab kasutajate regulaarse koolituse kahjurvaraga seotud võimalike ohte tuvastamiseks. On määratud protsess teavitamaks kahjurprogrammiga nakatumise kahtluse teavitamiseks.
Teenuseandja kohustused:
OPS.1.1.4.M5: Kahjurvaratõrje tarkvara rakendamine – teenuseandja testib kahjurvaratõrje tarkvara enne kasutuselevõttu, konfigureerib vastavalt keskkonnale ning piirab kasutajate õiguseid teha selles muudatusi.
OPS.1.1.4.M6: Viirusetõrjeprogrammide ja viiruse käekirja andmestike ajakohastamine – teenuseandja uuendab regulaarselt viirusetõrjeprogrammi ja viiruse käekirja andmestikke vastavalt tarkvara valmistaja soovitustele ning et uuenduste korral teeb vajadusel ka tarkvara konfiguratsioonis muudatusi.
Ühised kohustused:
OPS.1.1.4.M3: Kahjurvaratõrje tarkvara valimine lõppseadmetele – hankija annab hinnangu kahjurvaratõrje tarkvara valimiseks lähtuvalt kasutatavatest platvormidest, muudest olemasolevatest turvamehhanismidest, kahjurvaratõrje tarkvara eeldatavast jõudlusest ja avastusvõimest. teenuseandja võib konsulteerida.
ISKEs on kirjeldatud kõik OPS 1.1.4 meetmed. ISKE meetmed L ja M on E-ITSis kõrgmeetmete hulgas OPS.1.1.4.M10, OPS.1.1.4.M11, OPS.1.1.4.M12, OPS.1.1.4.M12, OPS.1.1.4.M13, OPS.1.1.4.M14, OPS.1.1.4.M15.

OPS.1.1.5: Logimine[32] – meetmed logiandmete turvaliseks kogumiseks, talletamiseks, analüüsimiseks ja nõuetekohaseks kõrvaldamiseks, täitmise eest vastutab IT-talitus
Hankija kohustused:

[31] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops1-oma-kaeidutoeoed/ops11-itpoohitoeoed/ops114-kaitse-kahjurprogrammide-eest/3-meetmed
[32] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops1-oma-kaeidutoeoed/ops11-itpoohitoeoed/ops115-logimine/3-meetmed

OPS.1.1.5.M1: Logimise eeskiri – hankija kehtestab logimise eeskirja. See hõlmab logimise planeerimist, korraldamist ja rakendamist, mis peavad olema kooskõlas infoturvapoliitikaga. Hankija kontrollib ka täitmist.

Teenuseandja kohustused:

OPS.1.1.5.M3: Sündmuste logimise konfigureerimine – teenuseandja konfigureerib sündmuste logimise. Teenuseandja peab tagama, et logimise eeskirjaga hõlmatud IT-süsteemides ja rakendustes on kasutusele võetud sisemised logimisfunktsioonid ning nende toimimist ja korrektsust kontrollitakse regulaarselt.

OPS.1.1.5.M4: Aja sünkroniseerimine – teenuseandja tagab kellade sünkroonimise logitavate IT-süsteemide ja rakenduste vahel, et logid oleksid ajaliselt täpsed.

OPS.1.1.5.M8: Logiandmete arhiveerimine – teenuseandja arhiveerib logiandmed vastavalt logimise eeskirjale ja asjakohastele õigusaktidele.

Ühised kohustused:

OPS.1.1.5.M5: Õiguslike raamtingimuste täitmine – hankija tagab logimisprotsesside andmekaitse ja muude asjakohaste õigusaktide järgimise nõudeid, teenuseandja rakendab protseduure.

OPS.1.1.5.M6: Keskse logitaristu rajamine – hankija loob keskse logitaristu strateegia eest, teenuseandjakuid rakendab ja haldab seda.

OPS.1.1.5.M9: Logiandmete valmendus analüüsimiseks – hankija määrab logiandmete arhiveerimise ja analüüsimise protseduurid, teenuseandja viib neid läbi.

OPS.1.1.5.M10: Logiandmete kaitse lubamatu juurdepääsu eest – hankija määrab logiandmete kaitse põhimõtted, teenuseandja rakendab ja haldab neid, sealhulgas tõkestab volitamata juurdepääsu.

ISKEs on kirjeldatud kõik OPS 1.1.5 meetmed. Sealhulgas ISKE meetmed L ja M on E-ITSis kõrgmeetmete hulgas: OPS.1.1.5.M11, OPS.1.1.5.M12, OPS.1.1.5.M12, OPS.1.1.5.M13.

OPS.1.1.6: Tarkvara testimine ja kasutuselevõtt[33] – tarkvara testimise ja kasutuselevõtu soovituslikud protseduurid ning meetmed kasutusele võetava tarkvara tehnilistele ja korralduslikele turvanõuetele vastavuse tagamiseks, täitmise eest vastutab IT-talitus

Hankija kohustused:

OPS.1.1.6.M1: Tarkvara testimise kavandamine – hankija määrab testimise raamtingimused, mis on kooskõlas kaitsetarbe ja tehniliste võimalustega, sealhulgas tagab testimiskeskkonna sarnasuse käidukeskkonnaga.

OPS.1.1.6.M4: Tarkvara kinnitamine – hankija kinnitav struktuuriüksus kontrollib tarkvara nõuetekohase testimise ja kinnitab selle kasutuselevõtu.

OPS.1.1.6.M6: Tarkvara testija juhendamine – hankija teavitab tarkvara testijat piisava ajavaruga ning tutvustab tarkvara kasutusviise ja täiendavaid nõudeid.

OPS.1.1.6.M10: Testimise vastuvõtu kord – hankija kehtestab testimise vastuvõtu korra, määratledes kohustuslikud testid, oodatavad tulemused ja testimise vastuvõtu kriteeriumid.

Teenuseandja kohustused:

OPS.1.1.6.M2: Tarkvara funktsionaaltestimine – teenuseandja vastutab tarkvara funktsionaaltestimise eest, kõiki tarkvara funktsioone kontrollitakse tarkvara funktsionaaltestimise käigus, veendumaks nende nõuetekohases toimimises.

OPS.1.1.6.M3: Testimistulemuste analüüsimine – teenuseandja analüüsib testimistulemusi, testitulemuste analüüsi käigus võrreldakse testimisel saadud tegelikke väärtusi oodatavate tulemustega ning dokumenteeritakse analüüsi tulemused.

[33] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops1-oma-kaeidutoeoed/ops11-itpoohitoeoed/ops116-tarkvara-testimine-ja-kasutuselevoott/3-meetmed

OPS.1.1.6.M11: Testandmete anonüümimine või pseudonüümimine – teenuseandja vastutab testandmete anonüümimise või pseudonüümimise eest, et kaitsmaks tundlikke andmeid.
OPS.1.1.6.M7: Personali valimine tarkvara testijaks – teenuseandja valib personaali tarkvara testijateks, tagab, et testijatel on vajalik erialane kvalifikatsioon ning teadmised kasutatavatest programmeerimiskeeltest, arenduskeskkondadest ja testimismeetoditest.
OPS.1.1.6.M13: Testkeskkonna lahutamine käidukeskkonnast – teenuseandja lahutab testkeskkonna käidukeskkonnast, et tagada tarkvara testimine vaid selleks ettenähtud keskkonnas ning vältida testimisest tulenevaid riske või häireid käidukeskkonnas.
OPS.1.1.6.M15: Paigaldamise ja seadistamise juhendi järgimine – teenuseandja valmistab ette tarkvara testkeskkonna vastavalt tarkvara paigaldamise ja seadistamise juhendile.
Ühised kohustused:
OPS.1.1.6.M5: Mittefunktsionaalsete testide tegemine – hankija ja teenuseandja teevad koostööd tarkvara jõudluse, kvaliteedinäitajate ja turvalisuse testimisel, kus teenuseandja viib läbi testid hankija määratletud ulatuses ja nõuetes.
OPS.1.1.6.M12: Regressioontestimine – hankija määratleb testimise nõuded ja protseduurid, teenuseandja viib läbi testimise.
ISKEs on kirjeldatud OPS 1.1.6 meetmest OPS.1.1.6.M1 ja OPS.1.1.6.M14. Sealhulgas ISKE meede M on E-ITSis kõrgmeetmete hulgas: OPS.1.1.6.M14.

DER.2.1 Turvaintsidentide käsitlus[34] – juhised turvaintsidentide süstemaatiliseks käsitlemiseks, täitmise eest vastutab infoturbejuht
Hankija kohustused:
DER.2.1.M1:Turvaintsidendi määratlemine – hankija määratleb, millised on organisatsiooni jaoks turvaintsidendid.
DER.2.1.M2: Turvaintsidentide käsitluse juhend – hankija on koostanud turvaintsidendi käsitluse protsessijuhendi ning ajakohastab seda.
DER.2.1.M4: Turvaintsidendist teavitamise kord – hankija on loonud korra teavitaks turvaintsidendist vajalikke asjaosalisi.
DER.2.1.M7:Turvaintsidentide käsitluse metoodika – hankija on dokumenteeritud metoodika ja protseduurid eri liiki turvaintsidentide käsitlemiseks. dokumenti ajakohastatakse regulaarselt.
DER.2.1.M9: Turvaintsidentidest teavitamise juhend – hankija koostab intsidentidest teavitamise juhendi.
DER.2.1.M10: Turvaintsidentide toime piiramine – hankija on koostanud kõige tõenäolisemate intsidendistsenaariumide jaoks intsidendi käsitlemise tegevuskava.
DER.2.1.M11: Turvaintsidentide hindamine – hankija on turbehalduse ja intsidendihalduse funktsioonidele kehtestatud ühtse protseduuri turvaintsidentide ja muude häiringute hindamiseks ja liigitamiseks.
DER.2.1.M12: Turvaintsidentide ja IT-intsidentide käsitluse ühendamine – hankija on analüüsinud turvaintsidentide ja IT-intsidentide kokkupuutekohti ning määratlenud vastavad kasutatavad ressursid.
DER.2.1.M13: Turbe- ja avariihalduse integreerimine – hankija vastutada.
DER.2.1.M14: Turvaintsidentidest teavitamise eskalatsiooniplaan – hankija koostab eskalatsiooniplaani egevusjuhistega, keda ja mis juhtudel intsidendi lahendamiseks täiendavalt kaasatakse. Hankija kaasajastab plaani.
DER.2.1.M16: Turvaintsidentide käsitluse dokumenteerimine – hankija on loonud tüüpprotseduuri turvaintsidentide dokumenteerimiseks.

[34] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/der-avastamine-ja-reageerimine/der2-turvaintsidentide-haldus/der21-turvaintsidentide-kaesitlus/3-meetmed

DER.2.1.M17: Turvaintsidentide järeltoimingud – hankija annab hinnangu turvaintsidentide käsitlemisele.
DER.2.1.M18: Protsessi täiustamine kogemuste ja välisarengute põhjal – hankija küsib tagasisidet turvaintsidentide lahendamisel kaasatud olnud isikutelt ja vastutajatelt. Hankija ajakohastab intsidentide avastamis- ja haldusvahendeid ning juhendeid.

Teenuseandja kohustused:

DER.2.1.M5: Turvaintsidendi lahendamise kord – teenuseandja vastutab turvaintsidendi lahendamise kordade eest, tal on vajalikud teadmised, ressursid ja juurdepääs süsteemidele, et kiiresti ja tõhusalt reageerida võimalikele turvaintsidentidele. Teenuseandjal on sageli spetsialiseeritud personaal ja tehnoloogilised vahendid, mis võimaldavad kasutusele võtta kiired ja tõhusad meetmed intsidentide lahendamiseks ning tagada teenuste ja andmete turvalisus.

Ühised kohustused:

DER.2.1.M3: Vastutuste ja kontaktisikute määramine – hankija ja teenuseandja on mõlemad määranud kes ja millistel alustel saab otsustada kriminalistikauuringu algatamise ning kasutajad on läbinud vastava koolituse. Mõlemad hoiavad oma vastavad kontaktid ajakohased.
DER.2.1.M6: Töökeskkonna taastamine pärast turvaintsidenti – teenuseandjaga koostöös eraldatakse intsidendist mõjutatud seadmed võrgust, vajadusel varundatakse andmed, võimalusel kontrollitakse mõjutatud seadme operatsioonisüsteemi ja kõiki rakendusi, paigaldatakse puuduvad turvapaigad ja uuendid. Hankija kontrollib intsidendi järgselt andmete õigsust ja terviklust. Teenuseandjaga veendutakse varundatud andmete taastamisel, et need ei ole turvaintsidendist mõjutatud.
DER.2.1.M8: Turvaintsidentide käsitluse töörühm – teenuseandjaga koostöös on moodustatud töörühm, millekoosseisu võidakse olenevalt intsidendi liigist muuta.
DER.2.1.M15: IT-talituse töötajate valmidus turvaintsidentide käsitluseks – hankija tagab töötajatele turvaintsidentide tuvastamiseks vajalikud vahendid ja kontroll-küsimustikud. Teenuseandja vastava vastutusega töötajad on tutvunud turvaintsidentide käsitluse juhendiga ning läbinud vajalike vahendite kasutamise koolituse.
ISKEs on kõik DER2.1 meetmed kirjeldatud. ISKE meetmed L ja M on E-ITSis kõrgmeetmete hulgas: DER.2.1.M19, DER.2.1.M19, DER.2.1.M20, DER.2.1.M20, DER.2.1.M21, DER.2.1.M21, DER.2.1.M22, DER.2.1.M22.

NET.3.2: Tulemüür[35] – meetmed tulemüüri või tulemüürisüsteemi turvaliseks hankimiseks, rajamiseks, konfigureerimiseks ja käitamiseks, turvameetmete täitmise eest vastutab IT-talitus

Hankija kohustused:

NET.3.2.M7: Tulemüüri avariijuurdepääs – hankija on teadlik protsessidest ja võimalustest avariijuurdepääsuks, teenuseandjale on tagatud võimalus füüsiliseks juurdepääsuks.
NET.3.2.M15: Tulemüüri hankimise kord – hankija määratleb tulemüüri valiku nõuded, mis on kooskõlas organisatsiooni infoturbepoliitikaga.
NET.3.2.M32: Tulemüüri avariivalmendus – hankija integreerib tulemüüri avariivalmenduse oma üldisesse avariivalmenduse plaani.

Teenuseandja kohustused:

NET.3.2.M6: Tulemüüri haldusliideste turve – teenuseandja vastutab, et tulemüüri haldusliidestele oleks võimalik ligi pääseda ainult määratud IP-aadressidelt või -vahemikust ning et haldusliidestele ei oleks juurdepääsu ebausaldusväärsetest võrkudest. Lisaks tagab

[35] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/net-voorgud-ja-side/net3-voorgukomponendid/net32-tulemueuer/

teenuseandja, et tulemüüri kohtvõrgu haldusühenduste protokollid on turvalised või kasutatakse alternatiivina eraldi haldusvõrku.
NET.3.2.M9: Tulemüüri logimine – teenuseandja logib tulemüüri olulised turvasündmused, sealhulgas haldusliidesesse sisselogimised, konfiguratsioonimuudatused, blokeeritud võrguühendustaotlused, ebaõnnestunud juurdepääsukatsed süsteemiressurssidele ning tulemüüriteenuste ja üldiste tulemüüri veateadete salvestused. Tulemüüri tehtud toimingud logitakse võimalusel automaatselt.
NET.3.2.M10: Killuründe tõrje paketifiltris – teenuseandja tõrjub IPv4 ja IPv6 protokollide killuründe paketifiltris.
NET.3.2.M22: Tulemüüri kellaaja sünkroniseerimine – teenuseandja sünkroniseerib tulemüüri kellaaja turvalise NTP-serveriga ning blokeerib kellaaja sünkroniseerimise muude väliste allikatega.
NET.3.2.M16: Turvaline P-A-P-struktuur (paketifilter-rakenduslüüs-paketifilter) – teenuseandja rajab turvalise P-A-P-struktuuri.
NET.3.2.M17: IPv4 või IPv6 desaktiveerimine – teenuseandja desaktiveerib IPv4 või IPv6 protokolli tulemüüri liideses, kui vastav protokoll ei ole võrgusegmendis kasutusel.
NET.3.2.M18: Tulemüüri haldusvõrgu eraldamine – teenuseandja korraldab tulemüüri haldamine eraldi haldusvõrgu kaudu.
NET.3.2.M19: UDP-tulva ja TCP SYN-tulva ning järjenumbri äraarvamise tõrje paketifiltris – teenuseandja vastutab UDP-tulva ja TCP SYN-tulva ning järjenumbri äraarvamise tõrje eest paketifiltris, kasutades paketifiltrit.
NET.3.2.M23: Tulemüüri seire ja seiretulemuste analüüs – teenuseandja vastutab tulemüüri seire ja seiretulemuste analüüsi eest, hõlmates tulemüüride jälgimist, logide analüüsi ning automaatse teavitamise seadistamist oluliste sündmuste korral.
NET.3.2.M24: Läbivaatused ja läbistustestimised – teenuseandja vaatab tulemüüri regulaarselt läbi ja testib teadaolevate turvaprobleemide suhtes ning dokumenteerib läbivaatuste tulemused, et tagada tulemüüri turvalisus ja vastavus turvanõuetele.

Ühised kohustused:

NET.3.2.M1: Tulemüüride turvajuhend – hankija koostab oma üldise turvapoliitika alusel tulemüüride turvajuhendi, mis on kooskõlas organisatsiooni vajaduste ja standarditega. Teenuseandja järgib juhendit, hankija kontrollib juhendi järgmist.
NET.3.2.M2: Tulemüürireeglid – hankija vastutab oma turvapoliitikale ja vajadustele vastavate tulemüürireeglite kehtestamise eest, teenuseandja rakendab ja haldab reegleid.
NET.3.2.M3: Sobivad filtreerimisreeglid paketifiltris – hankija määratleb filtreerimisreeglid, mida teenuseandja rakendab ja haldab.
NET.3.2.M4: Tulemüüri turvaline konfigureerimine – teenuseandja vastutab tulemüüri konfigureerimise eest, hankija omab kontrolli konfiguratsiooni vastamise eest organisatsiooni turvanõuetele.
NET.3.2.M14: Tulemüüri käidudokumentatsioon – hankija on teadlik ja nõustub teenuseandja koostatud turvalisust mõjutavate toimingutega, mille lisab oma käidudokumentatsiooniga.
ISKEs on kõik NET.3.2 meetmed kirjeldatud. ISKE meetmed L ja M on E-ITSis kõrgmeetmete hulgas: NET.3.2.M20, NET.3.2.M20, NET.3.2.M21, NET.3.2.M22, NET.3.2.M28, NET.3.2.M28, NET.3.2.M29.

CON.3: Andmevarunduse kontseptsioon[36] – juhised organisatsiooni andmevarunduse kontseptsiooni koostamiseks ja rakendamiseks andmete kaitseks, meetmete täitmise eest vastutab infoturbejuht

[36] https://eits.ria.ee/et/versioon/2022/eits-poohidokumendid/etalonturbe-kataloog/con-kontseptsioonid-ja-metoodikad/con3-andmevarunduse-kontseptsioon

Hankija kohustused:
CON.3.M1: Andmevarunduse mõjurite piiritlemine – hankija koostab varundatavate andmete registri ja määrab andmevarunduse mõjurid.
CON.3.M2: Andmevarunduseeskiri – hankija koostab andmevarunduseeskirja.
CON.3.M4: Andmevarundusplaanid – hankija koostab andmevarundusplaani, kaasa arvatud varunduse ja andmetaaste põhimõtted.
CON.3.M6: Andmevarunduse kontseptsioon – hankija koostab andmevarunduse kontseptsiooni ning kooskõlastab selle vastutajatega ning kontrollib rakendamist.
CON.3.M7: Sobiva andmevarundussüsteemi soetamine – hankija valib ja soetab sobiva andmevarundussüsteemi.
CON.3.M9: Tingimuste tagamine kaugvarunduseks – hankija tagab teenusetasemelepingu sõlmimise ja määrab tingimused tagamaks kaugvarunduse efektiivse ja turvalise toimimise.
CON.3.M15: Varunduse regulaarne testimine – hankija testib regulaarselt andmevarunduse toimimist ja varundatud andmete taastamist.
Teenuseandja kohustused:
CON.3.M12: Varunduseks kasutatavate andmekandjate turvaline säilitus – teenuseandja vastutab varunduseks kasutatavate andmekandjate turvalise säilituse eest hoides andmekandjaid lähtesüsteemist eraldi. Teenuseandja tagab andmete turvalise säilituse vähemalt nõutud andmesäilitustähtaegade ulatuses, mis tähendab, et varundusandmeid hoitakse turvaliselt ja juurdepääs nendele on piiratud vastavalt kehtestatud säilituspoliitikale.
Ühised kohustused:
CON.3.M5 Regulaarne andmevarundus – hankija määrab andmevarunduse regulaarsuse ja korralduse, teenuseandja järgib kehtestatud ajakava ja protseduure.
CON.3.M14: Varukoopiate turve – hankija määrab turvastandardid ja -nõuded, teavitab töötajaid korraldusest, teenuseandja järgib standardeid ja nõudeid.
ISKEs on kõik CON.3 meetmed kirjeldatud. ISKE meetmed L ja M on E-ITSis kõrgmeetmete hulgas: CON.3.M13, CON.3.M13, CON.3.M13.

Lisa 3 – Teenuseandjate intervjuude küsimused ja kokkuvõtted

Lisas 3 on esitatud intervjuu küsimused teenuseandjatele, mis olid kavandatud hõlmama erinevaid aspekte seoses riigihangete tehniliste kirjeldustega ning infoturbe standardite rakendamisega. Intervjueeritavatele saadeti enne intervjuud tutvumiseks planeeritavad küsimused ja kontrollnimekirjad, kuigi intervjuu käigus ei jõutud läbi käia kõiki esialgselt kavandatud küsimusi. Allpool on toodud planeeritud küsimused, intervjuude kokkuvõtted on üksikasjalikumad.

Intervjuude küsimused

1. Kuidas hindate viimase aasta jooksul avaldatud riigihangete kvaliteeti?
   Täpsustav küsimus: Riigihanke koostamisele eelnev turu-uuring – teie hinnangul, kas hankijad teevad neid piisavalt saamaks aru teenuseandja võimekusest?
2. Kui palju riigihangetes üldse turvameetmeid loetletakse?
3. Kuidas on turvameetmeted sõnastatud? Teksti vormis või viitena, mingil muul viisil?
   Täpsustav küsimus: Kas näete ebakõla meetmete kirjeldamises? Kui jah, siis millist?
4. Kas hankijad oskavad infoturbe nõudeid korrektselt kirjeldada? Milline on teie kogemus selles osas?
   Täpsustav küsimus: Kui kogemused on positiivsed, siis mida toote välja hea näitena? Kui kogemused on negatiivsed, siis mis võiks olla selle põhjenduseks?
5. Kuidas lähete hankele, milles on välja toodud üldine nõue, et teenus peab vastama E-ITSile?
6. Kuidas käitute, kui riigihankes on meetmetena nõutud midagi, mis on nähtavalt hankija vastutusvaldkonnas?
   Täpsustav küsimus: Mis saab, kui märkate neid meetmeid, kas tulevad täpsustavad küsimused hankijale?
   Täpsustav küsimus: Kui palju täpsustavad küsimused hankeprotsessi pikendavad?
7. Kui palju kontrollib arhitekt riigihangetes küsitud meetmete vastavust pakutavale teenusele?
8. Juhul kui on kokkupuudet olnud mõlemaga – Millised erisused on ISKE ja E-ITSi nõuete kirjelduses?
   Täpsustav küsimus: Kummale on lihtsam vastata? Miks?
9. Kui on kokkupuudet olnud ISO/IEC 27001 ja 27002-ga, millised erisused on nimetatud standardite ja E-ITSi nõuete ja kirjelduses riigihangetes?
10. Kas ja kui palju on kokkupuudet riigihangetes BSI IT-Grundschutz Compendiumiga?
11. Hinnang kontrollnimekirjadele: Mida te arvate sellest, kui hanke koostaja kasutaks kontrollnimekirju hankes olevate turvanõuete täpsustamiseks?
12. Kas kontrollnimekirjade juures tuleks midagi muuta? Kas midagi olulist on puudu? Kas näete kasutegurit oma töös, kui hankija nimekirju rakendanud?
13. Mida arvate kontrollnimekirjas olevatest üldistest nõuetest?
14. Mida arvate kontrollnimekirjas olevatest Kubernetese nõuetest?
15. Mida arvate kontrollnimekirjas olevatest veebiserveri nõuetest?

Telia Eesti AS

Intervjuus, mis toimus 15.03.2024 Telia kliendilahenduste peaarhitektiga arutleti IKT hankeseisu ja väljakutsete üle teenuseandja vaatenurgast. Intervjueeritav tõi välja hangete puuduliku kvaliteedi, mis võib olla tingitud vähesest hankele eelnevast turu-uuringust või ebamäärasest hangetingimuste kirjeldusest. Intervjueeritav tõi esile, et hankijate läbi viidavate turu-uuringute puudumine ning „teenus vastab E-ITSile” kirjeldus jätavad avamata võimaliku

meetmete spektri ja nendega kaasnevad kulud, mis omakorda võib põhjustada ebarealistlikke ootusi nii hankeobjekti maksumuse kui ka teostatavuse osas.

Intervjueeritav lisas, et hangete kirjeldustes ei ole muudatusi toimunud võrreldes E-ITSi ja ISKE meetmete kirjeldamisega. Arutelu keskmes oli hankijate vajaliku spetsiifilise ekspertiisi, nagu E-ITSi või ISKE standardite tundmise puudumine või vajalike ekspertide vähene kaasatus hankeprotsessis. Intervjueeritav tõdes, et see puudujääk viitab süsteemsele probleemile hankemenetluste ettevalmistamisel.

Intervjueeritav tõi välja, et hankemenetluste kirjelduste täpsustamine ja standardite parem mõistmine võib aidata vähendada ebakõlasid hankijate ja teenuseandjate vahel, luues selgema arusaama nõuetest ja vastavusest, kuna paljud teenuseandjad omavad ISO/IEC 27001 sertifikaati. Intervjueeritav lisas, et hankijal tuleks kasuks hankes soovitud meetmed ISO/IEC 27001 standardiga kokku viia. Intervjueeritav tõi välja, et mõnes hankes on ka E-ITS võrdsustatud ISO/IEC 27001-ga. Intervjueeritav lisas, et välismaised pakkujad ei pruugi olla kursis E-ITSiga.

Intervjueeritav selgitas, et tihti küsitakse lisadokumentatsiooni hankija käest kaitsmaks mõlema osapoole huve. Hanke täpsustavate küsimustega, mis üldiselt hankeprotsessi ei pikenda, proovitakse hankijale vajadusel märku anda, kui hankija soovib, et teenuseandja teostaks rolli, mis peaks olema hankija organisatsioonisisene, et selline vastutus ei ole majutaja või haldaja tagada. Samas peab intervjueeritav murekohaks täpsustavate küsimuste puhul vastaja rolli hankes – jurist, teenuse spetsialist või keegi teine, ning kuidas küsimusest aru saadi.

Intervjuus arutleti ka turu-uuringute olulisuse üle hankemenetluste parema struktureerimise ja läbipaistvuse saavutamiseks, mis aitaks mõlemal poolel paremini mõista hankeprotsessi ootusi ja võimalusi. Intervjueeritav lisas, et teenuseandja saab vastutada platvormi, keskkonna ja meetodite eest, aga rakenduse hästi kirjutamise eest vastutust võtta ei saa. Teenuse omanik hankijana omab teadmist, mis on teenuse sisu ning mis tüüpi andmeid milliste meetmetega kaitsta soovib.

Intervjueeritava soov arhitektina oleks, et enne teenuse käivitamist oleks tehtud test, kas teenus on ehitatud, arendatud soovitud turvameetmeid silmas pidades ning vajadusel tuuakse välja kitsaskohad, mida oleks vaja ringi teha – nõuete kontroll E-ITSi või ISO/IEC 27001 vaatenurgast hankeperioodi alguses, kas konfidentsiaalsus, terviklus ja käideldavus on vastav. Sellest kontrollist võivad välja tulla väga ebamugavad jääkriskid, mis on suur lisakulu, kuid ühtlasi hea ülevaade. Samuti suurendab see läbipaistvust.

Autori koostatud kontrollnimekirjade kohta leidis intervjueeritav, et rakenduse arenduse protsess võiks olla nimekirjas eespool – äripoole visiooni loomise ajal. Lisamärkusena ütles, et arenduse hangetel võiks kaasata kohe ka haldajat, et saaks anda arendajale oma sisendi anda. Intervjueeritav lisas, et arhitektuuriline joonis liideste koha pealt võiks samuti hankes kaasas olla – loogiline või protsessiline, kuna see annab ülevaate, mille turvalisust oodatakse.

Intervjueeritava seisukohalt teeb kontrollnimekirjade ja nende järgimine hanked kvaliteetsemaks – hankija teadvustab, mida soovib ja teenuseandja saab täpsemini vastata. Tabelite meetmete jagamise loogika märkusena tõi välja, et iga teenus on päeva lõpus natuke oma nägu, on võimatu luua mudel, mis kõigile sobib, kui 80% kattub, on juba väga hästi. Mõlemad tabelid täidavad selle kriteeriumi.

Intervjueeritav rõhutab, et toetavate teenuste puhul tagab teenuseandja rohkem meetmete rakendamist ning lisab, et kui hankija ise ei tea, mida soovib rakendada, siis on teenuseandjal raske vastata. Intervjueeritava arvamuse kohaselt tundub hetkel, et hankijad on mures, et kes vastutab ja igaks juhuks kirjeldavad turvameetmeid võimalikult laialt.

Primend OÜ

Intervjuu Primend OÜ IT-teenuste ärikonsultandiga toimus 27.03.2024 ning tõi esile mitmeid kriitilisi probleeme ja väljakutseid, millega IKT hangete kontekstis praegu silmitsi seistakse. Intervjueeritav rõhutas, et keskne probleem seisneb selles, et hankeprotsessid kipuvad keskenduma madalaimale võimalikule hinnale, jättes tähelepanuta teenuse kvaliteedi ja teenuseandja kompetentsi. Intervjueeritava sõnul ei soodusta selline lähenemine kvaliteetsete lahenduste pakkumist, arvestades, et hangete dokumentatsioon on sageli aegunud, mis peegeldab puudulikku arusaama kaasaegsest tehnoloogiast ja turvanõuetest.

Intervjueeritav osutab hanke protsessides esinevatele märkimisväärsetele lünkadele virtuaalkeskkondade ja nende asukoha sügavuti mõistmisel, rõhutades IKT valdkonna kiirele arengule. Intervjueeritav toob välja, et E-ITS ja ISKE näivad olevat kinni vananenud turvakäsitluses, mis keskendub rohkem füüsilisele perimeetrile kui andmete turvalisusele, mis on omakorda on muutunud oluliseks virtuaalkeskkondades ja pilveteenuste laialdasel kasutamisel. Intervjueeritav lisab, et on hädavajalik, et E-ITSi fookus oleks andmete turvalisus vastavalt IKT sektori arengule. Lisaks osutab intervjueeritav vajadusele üle vaadata riiklik poliitika, mis hetkel piirab avaliku pilve kasutamist, hoolimata sellest, et teatud lahendused, nagu näiteks Microsoft Exchange *on-premise*, on vananenud ega saa enam turvauuendusi. Selline lähenemine näib pidurdavat innovatsiooni ega pruugi kajastada praeguseid turvanõudeid ja -riske.

Intervjueeritav juhib tähelepanu olulistele aspektidele seoses rahvusvaheliste standardite ja E-ITSi vaheliste suhetega. Intervjueeritav tõdeb, et kuigi ISO/IEC 27001 standardi juurutamine pakub kuluefektiivset lähenemist ja rahvusvahelist tunnustust, nõuavad teatud teenused nagu näiteks X-tee ka E-ITSi rakendamist. Praegu valitseb arusaam, et ISO/IEC 27001 ja E-ITS on võrdsustatud, kuid see võib tulevikus muutuda ja selle pikaajalisuse osas valitseb ebakindlus. Intervjueeritav rõhutab, et üheks väljakutseks on E-ITSi asjakohaste ekspertide, nagu konsultantide ja audiitorite, puudus, kuna vastupidiselt ISO/IEC 27001 standardile, ei saa E-ITSi auditeerimiseks välismaiseid partnereid kaasata.

Intervjueeritav toob välja olulise aspekti seoses olemasoleva riigi infosüsteemiga, mis on ehitatud mingi turbetasemega ja võib-olla ei ole seda teenuseandjana võimalik turvalisemaks teha, kuna rakendus on võib olla vananenud (inglise keeles *legacy*). Intervjueeritav peab oluliseks, et teenuseandja, tema pakutav majutusruum, infrastruktuur ja spetsialistid peavad vastama mingile standardile. Ta leiab, et ISO/IEC 27001 sertifikaadi olemasolu peaks juba iseenesest tagama teenuseandja usaldusväärsuse, mistõttu ei näe ta vajadust lisada hankesse täiendavaid E-ITSi meetmeid ning lisab, et kui teenuseandja süsteemid ja protsessid on ISO/IEC 27001 standardiga kooskõlas, peaks see teoreetiliselt katma ka E-ITSi nõuded. Siiski tõstab ta esile, et hangetes, kus vastutusalad võivad jääda ebaselgeks, on kriitiline tähtsus vastutusvaldkondade selgitamisel ja täpsustamisel.

Intervjueeritav, olles teenuseandja, tunnistab oma vastutust dokumentatsiooni ajakohastamise suhtes. Ta märgib, et ei pruugi võtta initsiatiivi hankija vastutusvaldkonna poliitikate väljatöötamise eest, ka hankijate praeguste poliitikate olemasolu ja ulatus varieeruvad.

Protsessi käigus esitatavad täpsustavad küsimused ei pruugi tingimata pikendada hankeprotsessi, vaid võimaldavad paremini mõista teenuse vastavust kehtestatud nõuetele, eriti kui tellitav teenus on juba ISO/IEC 27001 teenuseandja seisukohast standardiga kooskõlas.

Autori koostatud kontrollnimekirjade kasutamine IKT hangete koostamisel lihtsustab intervjueeritava hinnangul vastutuse jaotust ja tegevuste määramist, pakkudes selgust ja hõlpsat mõistmist vastutusalade osas. E-ITSi juurutamine, kuigi finantsiliselt koormav, on põhjendatud, et tagada parimate praktikate järgimine ning vajaliku turvalisuse ja süsteemi uuenduste rakendamine. Seejuures rõhutab intervjueeritav, et vananenud tarkvara ja süsteemide, samuti elutsükli lõpuni jõudnud seadmete kasutamine nõuab uuendusi, et vastata nüüdisaegsetele turvanõuetele ning E-ITSi järgmise kohustus parandab ETOde küberturvet. Intervjueeritav leiab, et kontrollnimekirjad oleks suureks abiks ega leia, et oleks vaja midagi muuta. Tabelid tunduvad loogilised ja arusaadavad.

Intervjueeritav leiab, et E-ITSi implementeerimine organisatsioonil (eriti ETOdel) on kriitilise tähtsusega, et tagada IKT süsteemide turvalisus ja ajakohasus. Kuigi tegemist on lisakoormusega, mis nõuab järjepidevat investeeringut IT-infrastruktuuri, protsesside ja dokumentatsiooni, toetab see samal ajal organisatsioonide võimet vastata muutuvatele turvanõuetele ja -ohtudele, samas ebakindlus, koos kommunikatsioonilünkade ja kiirete juurutamisnõuetega suurendab organisatsioonidele tekkivat finantskoormust ja ajalist survet.

Tietoevry Estonia AS
Intervjuu leidis aset 03.04.2024 haldusteenuste osakonnajuhi ja lahenduste arhitektiga avades põhjaliku arutelu tehniliste kirjelduste ja dokumentatsiooni nõuete kohta IKT hangetes, tuues esile sektori väljakutsed ja lahendusvajadused. Intervjuus kerkib esile, et hangete tehnilistes kirjeldustes valitseb sageli tõlgendamisruumi, eriti kui on mainitud vajadust rakendada E-ITSi meetmeid, kuid ilma konkreetsete juhisteta, mida see rakendamine täpselt hõlmab.

Intervjuus käsitleti IKT hangete tehnilisi kirjeldusi ja dokumentatsiooni nõuete vastuolusid, mis toovad esile sektori ees seisvad väljakutsed. Nad tõid välja, et hangete tehnilistes kirjeldustes esinevad äärmused, kus mõnikord on nõuded loetletud detailse nimekirjana või on üldsõnaliselt mainitud, et lahenduses peab olema võimalik rakendada E-ITSi. Neil juhtudel, kui hankes on täpselt nimetatud meetmeid, saavad teenuseandjad konkreetsemalt aru, mida on vaja teha. Intervjueeritavad märkisid, et hangete sõnastuses on palju tõlgendamisruumi – üldine nõue „peab saama rakendada" on liiga pealiskaudne ega anna täpset ülevaadet sellest, mida hankija tegelikult ootab. Sageli ei kontrollita ka pärast hanke täitmist, kas ja kuidas on E-ITSi nõudeid rakendatud.

Intervjueeritavad tõstatasid olulise teema seoses projekti käivitamise ja juurutamisega IKT hangetes. Nad rõhutavad, et hangete juurutusfaasis peaks olema läbipaistvus klientide ja teenuseandjate vahel, et selgitada välja, kuidas on konkreetsete nõuete täitmine arhitektuuriliselt lahendatud. Tõdeti, et hankijatel on sageli vastumeelsus investeerida lisakuludesse, mis on seotud nõuete põhjaliku analüüsiga, kuna enamus hankeid keskenduvad peamiselt hinnale, E-ITSi kvaliteedi kontroll juurutamise käigus on tihti pealiskaudne ja selliseid aspekte ei ole hangetes piisavalt arvestatud. See sunnib hankijat kulutama oma aega ja ressursse, et tagada nõuete täitmine, mis võib mõjutada projekti üldist kvaliteeti ja edukust. Tõstatati küsimus, kuidas selline lähenemine, kus eelistatakse kiiremat ja odavamat lahendust, toetab pikemaajalist kvaliteeti ja vastavust turvanõuetele.

Lisaks tõid nad välja, et turu-uuringuid tehakse harva, mis tähendab, et hankijatel võib puududa selge arusaam turul saadaolevatest lahendustest ja nende vastavusest turvanõuetele. Hankeprotsessi pikkus ja keerukus võivad takistada sobiva lahenduse leidmist, mis vastaks nii kvaliteedi kui ka turvalisuse nõuetele.

Nad märkisid, et hangete dokumentides ei ole alati selgelt välja toodud, kellele kuulub vastutus teatud turvameetmete rakendamise eest, mis jätab ruumi tõlgendamiseks ja võib viia vastutuse ebaselguseni. Teenuseandjana peavad nad olema teadlikud oma kohustustest, kuid tihti on see info puudulik või ebaselge. Rõhutati ka ISO/IEC 27001 standardi rakendamise kohustust, mis lasub teenuseandjal endal. Intervjueeritavad tõid välja, et teenuseandjana peavad nad pakkuma nõuetekohase platvormi, kuid lõppkokkuvõttes on vajalik hankijal tellida auditeerimine, et veenduda nõuete täitmises. Intervjueeritavad juhtisid tähelepanu ka sellele, et hangete koostamisel ei pruugita alati arvestada oluliste aspektidega, mis viitab sellele, et strateegiline planeerimine võib olla puudulik või ei ole see läbinud organisatsiooni asjakohast osakonda. E-ITSi muutus kohustuslikuks alates 2023. aastast ning uute ettevõtete lisandumine, kellele kohustus laieneb, tähendab ka, et nende küpsusaste turvanõuete rakendamisel võib oluliselt erineda.

Intervjuus toodi välja, et kui hanke nõuded on kirjeldatud pealiskaudselt, annab see teenuseandjatele võimaluse tõlgendada nõudeid minimaalselt, keskendudes peamiselt hinnale. Hinnakriteeriumi puhul ilma täpsustuseta arvestatakse paratamatult hinna sisse nii vähe tööd kui vajalik, mis tekitab osakonnajuhis vastuolu nõuete ja tehniliste vajadusete kokku viimisel. Intervjueeritavad rõhutasid, et mõningad turvanõuded võivad olla juba arhitektuuriliselt tagatud, sõltumata sellest, kas klient neid spetsiifiliselt küsib või mitte. Sellega seoses tõid intervjueeritavad esile, kuidas ISO/IEC 27001 standardile vastavuse paljudel teenuseandjatel on aidanud täiendada organisatsioonilisi meetmeid, luues sellega teatud raamistiku, mis kitsendab tegevusi, mida teenuseandja peab spetsiifilise hanke jaoks tegema Nad rõhutavad, et teenuseandja valmidus ja küpsusaste teenuste käivitamisel mängivad suurt rolli selles, kuidas ja millises ulatuses nõudeid täidetakse.

Samuti kritiseerivad intervjueeritavad andmekaitse praegust seisukorda hangetes, märkides, et kuigi klientidelt küsitakse spetsiifiliselt andmekaitse lepinguid, on need tihtipeale üldsõnalised ja mitte väga põhjalikud. See sunnib neid teenuseandjana olema paindlik ja püüdma vastu tulla.

Intervjueeritavad tõdevad, et kuigi hangete nõuete kirjeldamine on muutunud täpsemaks tänu organisatsioonide teadlikkuse tõusule E-ITSi osas, ei pruugi see tingimata olla seotud üleminekuga ISKEst E-ITSile. Nad rõhutavad, et kui organisatsioon on varasemalt piisavalt vaeva näinud nõuete määratlemisega, muutub hangete kirjeldamine lihtsamaks ja korduvaks ülesandeks, mis aitab tagada sujuvama hankeprotsessi.

Intervjueeritavad rõhutavad oma intervjuus, et hankija organisatsioonil on valikuvabadus otsustada, kas rakendada E-ITS-i või rahvusvahelist ISO/IEC 27001 standardit. Teenuseandjana lähtuvad nad klientide vajadustest ja nõuetest. Intervjueeritavad toovad välja, et kuna nende organisatsioonil on juba ISO/IEC 27001 standard rakendatud, suudavad nad enamikus olukordades klientide vajadusi rahuldada, olles valmis vajadusel tegema lisajõupingutusi süsteemispetsiifiliste nõuete täitmiseks. Ühtlasi selgitavad intervjueeritavad, et ISO/IEC 27001 standardi kasutamine on eriti kasulik rahvusvahelises koostöös, kuna sellega ollakse väljaspool Eestit laialdasemalt kursis. See võib muuta koostöö allhankijatega lihtsamaks, eriti kui hangetes on esitatud E-ITSi nõuded, mis võivad nõuda „tõlget" või kohandamist, et rahvusvahelised partnerid neist aru saaksid.

Intervjueeritavad rõhutavad, kui oluline on hankijatel läbi mõelda ja täpsustada nõuded hangetes, et vältida tõlgendamisruumi ja tagada selge vastutusjaotus. Nad toovad välja, et kontrollnimekirjad ja konkreetselt määratletud vastutusalade läbimine aitab hankijatel paremini mõista, mida nad teenuseandjatelt ootavad, toovad hea näitena välja perearstikeskuste kui ka kohalike omavalitsuste jaoks loodud profiile. Lahenduse arhitekt kommenteerib Kubernetese tabelit ning tõstatab küsimuse vastutuse kohta tarneprotsessides, kus vastutaja määramine ei ole alati selge ning tarneprotsess võib kuuluda ka arendajale. Samas soovitavad mõlemad kasutada tabeleid, mis aitavad määratleda, kes mille eest vastutab, et hankija saaks selgelt aru, mida on õigustatud teenuseandjalt nõuda.

Intervjueeritavad rõhutavad, et hankija peaks E-ITSi või muude standardite rakendamisel arvestama konkreetsete vastutusaladega ja kaasama vajadusel konsultante, kes aitaksid vastutuse jaotamisel. Nad toovad esile, et vastutuse mõistmine ja harimine toimub sageli töö käigus, eriti konfliktiolukordades, mis sunnib organisatsioone oma lähenemist järgnevateks hangeteks kohandama.

Lõpetuseks rõhutavad intervjueeritavad, et riigiasutustes püütakse vältida sõltuvust ühest tarnijast (inglise keeles *vendor lock*), mis teeb oluliseks, et hangetes arvestataks vajadusega teenuseid tulevikus teistele pakkujatele üle anda. Lahenduse arhitekt soovitab kaaluda ja tulevikus näha ka E-ITSi vaates automatiseerimist ja standardiseerimist, näiteks kasutades skripte, mida saab riiklikult uuendada, et vähendada tõlgendamisruumi ja teha turbemeetmete rakendamise efektiivsemaks.

Lisa 4 – Hankijate intervjuude küsimused ja kokkuvõtted

Lisas 4 on esitatud intervjuu küsimused hankijatega, mis olid kavandatud hõlmama erinevaid aspekte seoses riigihangete tehniliste kirjeldustega ning infoturbe standardite rakendamisega. Intervjueeritavatele saadeti enne intervjuud tutvumiseks planeeritavad küsimused ja kontrollnimekirjad, kuigi intervjuu käigus ei jõutud läbi käia kõiki esialgselt kavandatud küsimusi. Allpool on toodud planeeritud küsimused, intervjuude kokkuvõtted on üksikasjalikumad.

Intervjuude küsimused

1. Palun kirjeldage eduka hanke protsessi?
2. Hanke koostamise protsess – millises mahus on sinna kaasatud E-ITSi meetmeid?
   Täpsustav küsimus: Kui suured on varasemad teadmised?
3. Kas organisatsioon on juba rakendanud E-ITSi või mõnda muud raamistikku?
4. Millise hinnangu annate enda organisatsioonis koostatud hangetele soovitud küberturbe meetmete kirjeldamise vaates?
   Lisaküsimus: Hanke koostamisele eelnev turu-uuring – kas teete neid? Kui teete – mille jaoks?
5. Kuidas sõnastate ise tellitavale teenusele rakenduvaid turvameetmeid – ehk milline on teie arusaam, parim praktika (parimad tulemused, vähem lisaküsimusi), kuidas need võiksid olla kirjeldatud hankedokumentatsioonis?
6. Kui sügavuti on hanke koostaja ise kursis organisatsiooni turbealase dokumentatsiooniga?
7. Kas organisatsioonil on turbelaane dokumentatsioon loodud?
   Täpsustav küsimus: Kas hanke koostamisel toetutakse sellele?
8. Kuidas on teie kogemused seoses infoturbe meetmete integreerimisega hankeprotsessi?
9. Kas näete ebakõla meetmete kirjeldamises? Kui jah, siis millist?
10. Kuidas on hankijana teie tunnetus – kui põhjalikult kontrollib teenuseandja soovitud meetmete sobivust hankele vastamisel?
11. Kui palju täpsustavad küsimused hankeprotsessi pikendavad?
12. Juhul kui on kokkupuudet olnud mõlemaga – Millised erisused on ISKE ja E-ITSi nõuete kirjelduses?
    Täpsustav küsimus: Kumba on lihtsam hangete kirjeldusse lisada? Miks?
13. Kui on kokkupuudet olnud ISO/IEC 27001 standardiga?
14. Millised erisused on ISO/IEC 27001 ja E-ITSi nõuete kirjelduses?
15. Kas ja kui palju on kokkupuudet hangetes BSI IT-Grundschutz'iga?
16. Hinnang kontrollnimekirjadele – Mida te arvate hanke koostajana, kui kasutaksite kontrollnimekirju hankes olevate turvanõuete täpsustamiseks?
17. Kas kontrollnimekirja juures tuleks midagi muuta? Kas midagi olulist on puudu?
    Täpsustav küsimus: Kas näete kasutegurit oma töös?
18. Mida arvate kontrollnimekirjas olevatest üldistest nõuetest?
19. Mida arvate kontrollnimekirjas olevatest Kubernetese nõuetest?
20. Mida arvate kontrollnimekirjas olevatest veebiserveri nõuetest?
21. Kas võtaksid selle juhendi aluseks, et edaspidi määrata hankeks vajalikke nõudeid?
    Täpsustav küsimus: Kui jah – millises mahus, kui ei – miks mitte?

Tallinna strateegiakeskus

Intervjuu Tallinna Strateegiakeskuse osakonnajuhiga toimus 05.04.2024, intervjueeritav tegeleb arvuti töökohateenuste ja seadmete sisseostuga. Intervjueeritav räägib, et kuigi seadus

nõuab E-ITSi rakendamist, on nad ise selles vallas alles algjärgus. Ta tõdeb, et kuigi infoturbepoliitikad ja käsikirjad on loodud, on praktikas veel palju tegemata ja lisab, et E-ITSi projektijuht on ametisse nimetatud. Intervjueeritav märgib, et kuigi nad on teinud suuri edusamme dokumentatsiooni osas, seisavad nad silmitsi väljakutsetega praktilise rakendamise tasandil.

Intervjueeritav räägib, et viimased hanked viitasid vanemale ISKE süsteemile ja selle turvaklassidele, need hanked jäävad veel eelmisesse aastasse, uutes hangetes jäetakse suur vastutus E-ITSi nõuete täitmise osas teenuseandjale, teenusekasutajana on nende jaoks oluline, et on kindlaks tehtud, et teenuseandja järgib E-ITSi. Intervjueeritava sõnul on E-ITSi rakendamine nii organisatsiooni kui ka teenuseandjate jaoks huvitav väljakutse, mis nõuab pidevat tähelepanu ja koostööd, et tagada turvanõuete täitmine ja andmekaitse tõhusus. Intervjueeritav tõi esile, et nende poolt koostatud hanked on väga detailsete kirjeldustega, eriti teenuste hangete osas. Siiski märkis ta, et turvalisuse aspektis võiks kirjeldused olla veelgi täpsemad. Praegu määratakse endiselt veel ISKE turvaklassid, kirjeldused ei ole läinud veel nii detailsesse tasandisse, näiteks konkreetsete E-ITSi meetmete kirjeldamiseni, samas tarkvara arenduse hangetes on edusamme tehtud.

Auditeerimise küsimus on intervjueeritava jaoks veel lahtine. Ta toob välja, et ei ole veel selge, kuidas nad hakkavad nõudma teenuseandjatelt infovarade vastutajate detailsust ja meetmete kontrolli raporteerimist. Intervjueeritav tõstatab küsimuse, kas audiitorid keskenduvad ainult sellele, et teenuseandjalt on info meetmete kohta küsitud või soovivad nad ka sügavamale süsteemi sisse vaadata, et olla teadlik nõuete täielikust järgimisest.

Intervjueeritavaga käsitleti IKT teenuste sisseostmise ideed ja protsesse, rõhutades ideaalseid tingimusi, kus turvanõuete järgimist kontrollitakse jooksvalt tarne käigus. Intervjueeritav räägib, et sisseostmise peamine põhjus on sageli organisatsiooni enda võimekuse puudumine teatud valdkondades, eriti administraatori tasandi ülesannetes, mis nõuavad spetsiifilisi teadmisi ja oskusi. Intervjueeritav selgitab, et hankeprotsessis on tavaliselt mitu vastutavat rühma: üks grupp vastutab tehnilise kirjelduse eest, teine viib läbi protsessi, sealhulgas viib läbi ka hanke väljakuulutamise ja protseduurilise raamistiku loomise. Tehnilise sisu eest vastutavad spetsialistid panevad kokku tehnilised lähteülesanded, samas kui õigusliku raamistiku ja hankeprotseduure kujundavad teised inimesed. Pärast pakkumiste esitamist osalevad hindamisel nii tehnilised kui ka mittetehnilised isikud.

Intervjueeritav toob esile, et elluviimise ajal ei pruugita alati kontrollida, kas teenused on käivitatud täpselt nii, nagu hankedokumentides nõutud, eriti kui tegemist on usaldusväärsete teenuseandjatega ning lisab, et probleemid ilmnevad tavaliselt siis, kui miski jääb puudu. Kui hangetes nõutakse täiendavaid meetmeid, muutuvad dokumendid pikemaks ja hankijale tekib vastuvõtmise ajal ka kontrollimise kohustus. Intervjueeritav märgib, et auditeerimine on loogiline samm, ja selline õigus peaks olema hankesse kirjutatud, kuid jääb küsimus, millises faasis auditeerimine toimub ja kes peaks kontrolli teostama. Kas see peaks olema tehnilise kirjelduse koostaja või infoturbe ekspert?

Intervjueeritav rääkis ka vajadusest, et ettevõttel peavad olema sisemiselt rakendatud teatud standardid ja protsessid peavad olema korrastatud, mis on eelduseks, et teenuseandjad saaksid kvaliteetselt teenuseid pakkuda. Ta tõstatas küsimuse, kas ja kuidas peaks tulevikus E-ITSi meetmeid hangetes kirjeldama, viidates vajadusele selles osas veel selgusele jõuda. Intervjueeritav märkis, et hangete koostamisel vaadatakse sageli, kuidas on sarnastes olukordades toimitud teised organisatsioonid, ja kui näiteks üks organisatsioon kirjeldab oma

nõudeid väga detailselt, võib see mõjutada ka teisi organisatsioone sarnaselt toimima. Lisaks mainis intervjueeritav, et järgmised suuremad hanked tulevad alles mõne aasta pärast, see annab neile aega E-ITSi täielikult rakendada ja saada rohkem kogemusi ISMSi rakendamises. Ta rõhutas, et järjepidevus ja varade vastutajate võime oma teenusele rakendatavad turvameetmed dokumenteerida on kriitilise tähtsusega, et tagada andmeturbepoliitika ja -meetmete tõhusus.

Intervjueeritav rõhutas, et kui teenuseandja esitab hankele vastates turvameetmete kohta küsimusi, on see märk sellest, et nad on pühendunud nõuete täitmisele. Ta tõi välja, et pakkumise dokumentatsioonis kirjeldavad teenuseandjad üksikasjalikult, kuidas nad on taganud nõuetele vastavuse, mis kinnitab, et teenuseandjad on turvanõuetele mõelnud ja need oma pakkumistes arvesse võtnud. Intervjueeritav märkis, et täpsustavad küsimused ei pikenda tavaliselt hankeprotsessi, kuna tellijana reageerivad küsimustele kiiresti ja asjakohaselt. Intervjueeritav nentis, et kuigi praegu probleeme pole, võib tulevikus E-ITSi nõue piirata välismaiste pakkujate osalemist Eesti hangetel, eriti tarkvara arenduse valdkonnas.

Kontrollnimekirjade tagasiside – intervjueeritav leiab, et kontrollnimekirjad on väga head ja nendest on kasu. Ta kiitis kasutatavaid nimekirju ja tabeleid, mis aitavad hankeprotsesse struktureerida ja dokumenteerida. Intervjueeritav märkis, et talle meeldib olemasolev ülesehitus, kuid tõi välja, et see tuleb kohandada vastavalt organisatsiooni küpsusastmele, mis võib nõuda dokumentide lühendamist või detailsemaks muutmist sõltuvalt, kui kaugele on hankija jõudnud E-ITSi rakendamisega.

Intervjueeritav tunnistas, et tunneb end justkui teekonnal, kuna E-ITSi täielik rakendamine on veel pooleli. Ta soovitas vaadata Strateegiakeskuse viimaseid tarkvara arenduse hankeid kui näidet selle kohta, kuidas turvameetmed on seal kirjeldatud. Ta rõhutas, et tabelid on loogilised ja aitavad oluliselt kaasa hangete selgusele ja arusaadavusele, aidates seeläbi tagada, et kõik hankes osalejad mõistaksid nõudeid ja ootusi.

Riigimetsamajandmise keskus

Intervjueeritav toimus 12.04 Riigimetsamajandamise keskuse infoturbe juhiga, kes räägib, et ta ei ole seni hangetes osalenud viisil, mis nõuaks spetsiifiliste infoturbe raamistike rakendamist, seega tunneb, et ei pruugi olla parim isik sel teemal arvamust avaldama. Praegu on ta hõivatud ISO/IEC 27001 auditi hanke ettevalmistamisega, kus tema vastutusalasse kuulub tehniline kirjeldus, samal ajal kui lepingu osa koostab õigusosakond. Ta tõi välja, et RMK, olles ainulaadne riigiasutusena tegutsev tulundusühing Eestis, ei ole varasemalt kohaldanud ISKE või muid sarnaseid infoturbe standardeid, mistõttu pole nende hangetes konkreetseid turvameetmeid või raamistikke kasutusele võetud. Intervjueeritav rõhutab, et kuna RMK-l puudub kogemus kindlate turbe raamistike rakendamisel, on tema roll välja töötada lähenemisviis praegusest IT-alasest olukorrast lähtuvalt, mida on varasemate süsteemsete raamistike puudumise tõttu vajalik arendada.

Intervjueeritav arutleb ISO/IEC 27001 standardi rakendamise lihtsuse üle, märkides, et see ei nõua suuri muutusi olemasolevas süsteemis, kuigi standardi kasutusele võtmine nullist võib olla keeruline ilma eelneva praktikata. Ta toob välja, et teenuseandjatel võib olla raske vastata erinevate organisatsioonide poolt erinevalt esitatud nõuetele. Intervjueeritav rõhutab, et on oluline mõista, kuidas need nõuded raamistikku sobitada, ning peab seda väärtuslikuks tööks.

Intervjueeritav mainib, et on organisatsioone, mis sarnaselt RMK-le varem ei ole pidanud küberturbe seadusi järgima ja kelle küpsustase turvalisuse osas võib olla madal. Ta leiab, et

olemasoleva süsteemi täiustamine on lihtsam kui uue süsteemi loomine algusest. Ta on täheldanud, et varasemates hangetes kirjeldatud mittefunktsionaalsed nõuded ei pruugi alati vastata standarditele ega ole alati piisavad, mis viitab vajadusele neid üle vaadata. Intervjueeritav tõdeb, et mittefunktsionaalsete nõuete loetelu on sageli koostatud erinevatest ISO/IEC 27001 ja E-ITSis toodud nõuetest. Praegu on tema ülesandeks luua organisatsiooni küberturbe alast dokumentatsiooni, mis aitaks paremini struktureerida ja määratleda turvanõudeid.

Intervjueeritav arutleb E-ITSi ja ISO/IEC 27001 standardite rakendamise üle, rõhutades, et nende esmane nõue on infoturbepoliitika olemasolu. Ta toob esile raskuse selles, et organisatsioonil peab olema ühtne arusaam turbe lähenemisest, et efektiivselt poliitikat luua. Ta kritiseerib poliitika loomist ilma ettevalmistava tööta alampoliitikate ja korralduste näol, mis teeb poliitika üldsõnaliseks ja ebaefektiivseks. Lisaks puudutab ta standardite laiemat rakendamist organisatsiooni protsessides, sealhulgas tarnesuhete haldust, mis on kriitilise tähtsusega, kuid veel ei ole lõplikult välja arendatud. Intervjueeritav rõhutab, et standardite rakendamine on keeruline ja aeganõudev protsess, mis nõuab põhjalikku lähenemist kõigile organisatsiooni aspektidele, alates äriprotsessidest kuni ITILi protsessideni. Ta toonitab, et see töö ei ole lihtsalt formaalsus, vaid nõuab tõelist pühendumist ja mõistmist, kuidas turvanõuded organisatsiooni töösse integreerida.

Intervjueeritav peab oluliseks, et dokumente ei loodaks ainult dokumentide pärast, vaid et need aitaksid kaasa reaalsetele muudatustele organisatsiooni turbepraktikates. Ta on mures väikeste organisatsioonide võime pärast rakendada samu nõudeid, mis on kehtestatud suurematele, arvestades ressursse ja olemasolevat infrastruktuuri.

RMK, mis ei ole varem Eesti infoturbestandardeid rakendanud, järgib mitmeid ISO standardeid, mis on kooskõlas nende põhitegevustega nagu metsamajandus ja looduskaitse. RMK rahvusvahelised partnerid on rohkem kursis ISO/IEC 27001 standardiga kui E-ITSiga, mis võib olla vähem tuntud väljaspool Eestit. Intervjueeritav, arutades mõlema standardi rakendamist, märgib, et ISO/IEC 27001 jätab organisatsioonidele vabaduse otsustada, kuidas nõudeid täita, samas kui E-ITS pakub täpsemaid juhiseid, mis on kasulikud neile, kellel puudub varasem kogemus. Ta tõstab esile ka E-ITSi uuendamise vajadust, mis toob kaasa halduskoormuse. Samuti mainib ta audiitorite puudust seoses kasvava nõudlusega.

Intervjueeritav arutleb, et kontrollnimekirjad, mille kontekst ja vajadus on hästi välja toodud, keskendub siiski ainult kahele teenusele: Kubernetes ja veebiserver. Ta leiab, et üldosa kontrollnimekirjast ei mõju küsimustikuna piisavalt terviklikult. Intervjueeritav täpsustab, et kuigi kontrollnimekirjad on kasulikud, piirdub see selgelt ainult kahe teenuse hankimisega ja võiks hõlmata laiemat teenuste spektrit. Ta tõstab esile kontrollnimekirja potentsiaali selgitada hangete nõudeid selgemalt, et vältida hangete venimist. Siiski märgib ta, et nõuete liiga üldsõnaline esitamine võib tekitada teenuseandjates segadust ning neil võib tekkida küsimusi, kuidas nõudeid täpselt täita. Intervjueeritav soovitab, et nimekirjas võiks olla detailsemad kirjeldused nõutavate meetmete osas, sealhulgas millises meetmeklassis need asuvad ja mida täpselt rakendada soovitakse, et tagada suurem selgus ja vastutuse selge jaotumine hangetes.

Eesti Raudtee

Intervjuu toimus 12.04.2024, IT osakonna juhataja ja infoturbe juhiga. Eesti Raudtees on kasutusele võetud ISO/IES 27001 standard. Infoturbealaste hangete koordineerimise eest vastutab spetsiaalne osakond, kus kõik tehnilised nõuded peavad saama infoturbe juhi heakskiidu. IT osakonna juht rõhutab, et hankes oluline aspekt on sertifikaadi olemasolu, kuid

tegelik kontroll on harv. Ta lisab, et rahvusvaheliselt on tavaline, et hankijal on õigus nõuda CIS 20 meetmete alusel auditit, mis tõendab turvanõuete täitmist. GDPRi raames peab Eesti Raudtee veenduma, et volitatud töötlejad täidavad oma kohustusi. Infoturbe juht toob esile, et suuremate hangete puhul nõutakse ISO/IEC 27001 standardi või samaväärse rakendamist, kuid tunnistab, et E-ITSi standardi põhjalik tundmine on keeruline, kuna see nõuab paljude meetmete tundmist. Viimastes hangetes on esitatud nõue, et teenuseandjal peab olema ISO/IEC 27001 sertifikaat või ta peab selle esitama aasta jooksul. Lisaks töötatakse välja mittefunktsionaalseid nõudeid, et maandada infoturbe riske, kuid paljudes kohtades pole varem infoturbe nõudeid olnud, mis raskendab nende teenuseandjatelt nõudmist. Oma ISO/IEC 27001 sertifikaat on olemas ja infoturbe dokumentatsioon on paigas.

Intervjueeritavad selgitavad standardite rakendamist: ISO/IEC 27001 puhul tuleb järgida kirja pandud protsesse, kuid standard lubab juhatusel aktsepteerida teatud meetmete mittetäitmist, ISO/IEC 27001 eeldab, et vähemalt 80% meedetest on täidetud. E-ITS nõuab samuti teatud meetmete täitmist, kuid võimaldab ka tuumikmeetmete mittetäitmist erijuhtudel. Osakonnajuht toob välja, et Eesti Raudtee nõuab ISO/IEC 27001 järgimist kõikides hangetes, eriti arendustööde puhul, kus riskid on suuremad ja nõuded detailsemad.

Väiksemate teenuseandjate suhtes pole seni turvanõudeid karmilt kehtestatud, mis võib kujuneda probleemiks, kuna turvanõuete eeldamine ei pruugi alati tagada piisavat kaitset. Osakonna juht toob välja, et tarkvara hankimisel kasutatud sertifikaatide nõue aitas suurendada turvameetmete rakendamist, motiveerides organisatsioone järgima rahvusvaheliselt tunnustatud standardeid.

Infoturbe juht sõnas, et Eesti Raudtee valis ISO/IEC 27001 standardi 1,5 aastat tagasi, kuna see on paindlik ja rahvusvaheliselt tunnustatud, mis on oluline ettevõtte paljude välismaa partnerite tõttu. E-ITS, mis on pigem standard, see ei ole välispartneritele tuntud, mistõttu peaks Eesti Raudtee rakendamisel suutma tõlkida E-ITS nõuded ISO/IEC 27001 keelde, mis oleks suur investeering.

Intervjueeritavad arutlevad E-ITSi ja ISO/IEC 27001 standardite eripärade ja nende rakendamise üle. Infoturbe juht rõhutab, et E-ITSi rakendamine võib tagada ISO/IEC 27001 standardi nõuete täitmise, kuid vastupidine olukord on keeruline, kuna ISO/IEC 27001 ei nõua organisatsioonilt protsesside muutmist, vaid pigem nende dokumenteerimist selliselt, nagu need juba toimivad. Seevastu E-ITS nõuab protsesside kohandamist vastavalt standardi nõuetele, mis võib tema hinnangul kaasa tuua riske. Osakonna juht toob esile, et E-ITS keskendub traditsioonilistele *on-premise* lahendustele, mis ei pruugi olla piisavad kaasaegses IT-maastikus, kus teenused ja andmed asuvad sageli pilves. E-ITSi piirangud pilveteenuste ja kaasaegsete IT-praktikate osas võivad viia valekindlustunde tekkimiseni, kus turvameetmete rakendamine ei kata tegelikke riskikohti. Mõlemad tunnistavad ISO/IEC 27001 paindlikkust kui väärtust, mis võimaldab standardit kohandada vastavalt tehnoloogia arengule ja organisatsiooni spetsiifikale, pakkudes seeläbi pikaajalist ja kohandatavat lähenemist turvalisuse tagamisel.

Intervjueeritavad arutlevad kontrollnimekirjade ja nende rakendamise üle turvameetmete osas, viidates erinevatele standarditele ja meetoditele nagu OWASP ja CIS 20 tase kaks. Infoturbe juht näeb, et kontrollnimekirju võiks rakendada lihtsamalt, keskendudes kaitsetarbele ja spetsiifilistele nõuetele. Osakonna juht rõhutab, et vastutusalad hangetes ja teenuste pakkumisel ei pruugi alati olla ilmselged, toob näiteks TLS krüpteerimise, mis on teenuseandjate, nagu Cloudflare, kaudu sageli eelseadistatud. Kui lahendus on ise koostatud,

näiteks kasutades infrastruktuuri kui teenust (IaaS), siis teenuseandjal võib olla ainult piiratud roll.

Nad arutavad ka seda, et teenuseandja ja hankija vastutusalad on tihti segased, mis nõuab mõlemalt poolelt selgete ootuste ja vastutuste määramist. Infoturbe juht leiab, et hankijad peaksid võib-olla kasutama teisi raamistikke, mis katab E-ITSi nõuded paremini ja seab vastutuse rohkem hankijale. Osakonna juht toonitab, et hankeprotsessis peab olema selge, mida teenuselt oodatakse, et tagada mõlema osapoole vahel usalduslik ja mõistev suhe.

Nad mõlemad nõustuvad, et kontrollnimekirjad on kasulikud, kui need sisaldavad selgeid juhiseid ja auditeerimise õigust, arvestades teenuste eripärasid. Osakonna juht soovitab kontrollnimekirjade kasutatavust, kui on nõutud CIS 20 nõuded, mis aitaksid tagada teenuste kvaliteedi ja turvalisuse.

I. Litsents

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, **Kadri Koit**,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose

„Eesti infoturbe standardi (E-ITS) nõuete kirjeldamine riigihangetes“

mille juhendaja on Kristjan Krips,

reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Kadri Koit

15.05.2024