TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Anti Allikvee 242776IVCM

Assessing the Administrative Implications of Estonian Regulatory Information Security Framework

Master's Thesis

Supervisor: Kaido Kikkas
PhD

Tallinn 2026

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Anti Allikvee 242776IVCM

Eesti regulatiivse infoturbe raamistiku administratiivsete mõjude analüüs

Magistritöö

Juhendaja: Kaido Kikkas
PhD

Tallinn 2026

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis and that this thesis has not been presented for examination or submitted for defence anywhere else. All used materials, references to the literature, and work of others have been cited.

Author: Anti Allikvee

14.05.2026

Abstract

This thesis examines Estonian regulatory information security framework by focusing on the information obligations it prescribes. It focuses on the structure, type, and cumulative logic of documentation, reporting, storage, updating, and related formal requirements, and on what these reveal about the framework's administrative design, internal coherence, and likely burden.

The study is based primarily on qualitative document analysis of legal acts, explanatory materials, guidance documents, and related supporting sources within Estonian regulatory information security framework. The Standard Cost Model informs it in a qualitative and analytical form. The aim is not to calculate exact compliance costs, but to provide a structured account of the administrative implications of information obligations at the framework level.

The analysis shows that the framework is broad, layered, and strongly documentary in character. The mapping identified 639 information obligations and 164 uniquely named documentary artefacts across the analysed legal sources. These findings indicate that the framework operates through much more than direct reporting duties to the state. It creates a wider documentary environment of policies, plans, registers, procedures, records, and audit-related materials that organisations must create, maintain, interpret, and demonstrate over time.

The thesis also shows that concerns about readability, documentation workload, audit capacity, and cumulative burden were visible during the framework's legislative development. However, they were only partly reflected in formal impact assessments. The findings suggest that Estonian regulatory information security framework functions as a documentary compliance regime. Administrative pressure arises from documentary formalisation, interpretive complexity, uneven organisational capacity, and cumulative

regulatory growth. On that basis, the thesis offers practical recommendations for improving terminological coherence, reducing duplication, clarifying documentary expectations, and strengthening implementation support.

The thesis is in English and contains 42 pages of text, 8 chapters.

Annotatsioon

Eesti regulatiivse infoturbe raamistiku administratiivsete mõjude analüüs

Käesolev magistritöö analüüsib Eesti kehtivat infoturbe raamistikku selles kehtestatud dokumenteerimiskohustuste kaudu. Töö keskendub dokumenteerimis-, aruandlus-, säilitamis-, ajakohastamis- ja muude formaalsete nõuete struktuurile, tüübile ja loogikale. Samuti uuritakse, mida need näitavad raamistiku ülesehituse, sisemise sidususe ja tõenäolise administratiivkoormuse kohta.

Uurimus põhineb peamiselt kvalitatiivsel dokumendianalüüsil, mille allikateks on Eesti infoturbe raamistiku õigusaktid, seletuskirjad, juhendmaterjalid ja muud seotud dokumendid. Analüüs lähtub Standard Cost Modeli loogikast kvalitatiivses ja analüütilises vormis. Eesmärk ei ole arvutada välja täpseid nõuete täitmise kulusid, vaid anda struktureeritud ülevaade sellest, milliseid administratiivseid mõjusid sellised nõuded raamistiku tasandil kaasa toovad.

Analüüs näitab, et Eesti infoturbe raamistik on lai, mitmekihiline ja tugevalt dokumentatsioonikeskne. Kaardistus tuvastas analüüsitud õigusallikates 639 dokumenteerimisega seotud kohustust ning 164 unikaalse nimetusega dokumentaalset artefakti. Need tulemused osutavad, et raamistik ei toimi üksnes otseste riigile suunatud aruandlusnõuete kaudu. See loob laiema dokumentidest koosneva keskkonna, mis sisaldab poliitikaid, plaane, registreid, protseduure, kirjeid ja auditiga seotud materjale. Paljusid neist peavad organisatsioonid aja jooksul looma, hoidma, tõlgendama ja vajaduse korral nende olemasolu tõendama.

Töö näitab, et murekohad seoses normide loetavuse, dokumenteerimiskoormuse, auditivõimekuse ja suurenava halduskoormusega olid nähtavad juba õigusloome käigus, kuid formaalsetes mõjuhinnangutes kajastusid need vaid osaliselt. Kokkuvõttes viitavad

tulemused sellele, et Eesti infoturbe raamistik toimib dokumentaalse vastavusrežiimina, milles halduskoormus tuleneb dokumenteerimiskohustustest, tõlgenduslikust keerukusest, organisatsioonide ebaühtlasest võimekusest ning regulatiivsete nõuete ajas kuhjumisest. Nendele järeldustele tuginedes pakub töö praktilisi soovitusi terminoloogia ühtlustamiseks, dubleerimise vähendamiseks, dokumenteerimisootuste täpsustamiseks ning rakendamistoe parendamiseks.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 42 leheküljel, 8 peatükki.

List of abbreviations and terms

BSI	Federal Office for Information Security, Germany
EIS	Eelnõude infosüsteem
E-ITS	Eesti infoturbestandard
EU	European Union
FQ	Focus question
GDPR	General Data Protection Regulation
ICT	Information and communication technology
ISKE	Infosüsteemide kolmeastmeline etalonturbe süsteem
ISMS	Information Security Management System
IT	Information technology
ITL	Eesti Infotehnoloogia ja Telekommunikatsiooni Liit
KTN	Võrgu- ja infosüsteemide küberturvalisuse nõuded
KüTS	Küberturvalisuse seadus
NIS	Directive on security of network and information systems
NIS2	Updated NIS directive
RIA	Riigi Infosüsteemi Amet
RIHA	Riigi infosüsteemi haldussüsteem
RQ	Research question
RT	Riigi Teataja
TalTech	Tallinn University of Technology

Table of contents

1. Introduction

Estonia is widely recognised as a leader in digital governance, with a strong commitment to secure and efficient digital services. This development has been accompanied by an expanding regulatory environment in which cybersecurity governance is increasingly structured through formal requirements, documentation, and compliance obligations.

1.1 Background and motivation

Estonia is widely recognised for digital governance and for its reliance on secure digital services. As digital dependence has increased, cybersecurity regulation has become a more significant part of public governance. These regulatory frameworks do not only establish security objectives. They also structure organisations through formal requirements concerning information, documentation, accountability, and demonstrable compliance.

Such requirements may support oversight, coordination, and consistency. At the same time, they require time, expertise, and administrative effort. Their implications are therefore not limited to technical security implementation, but also extend to the organisational work needed to understand, document, maintain, and demonstrate compliance.

This creates a need to examine Estonian regulatory information security framework not only as a legal framework, but also as a structure of information obligations. The central motivation of this thesis is to analyse what kinds of information obligations the framework imposes, how those obligations are structured, and what their likely administrative implications are at framework level.

1.2 Problem statement and research questions

The research problem of this thesis arises from the growing role of documentation, reporting, and other formal information obligations in cybersecurity regulation. While such obligations may be justified as tools of accountability and risk governance, they may also generate cumulative administrative demands that are not always visible when requirements are viewed separately.

The goal of the thesis is to examine Estonian regulatory information security framework as a whole through the information obligations it prescribes. The thesis focuses on the structure, type, and cumulative logic of those obligations and on what they reveal about the framework's administrative design, internal coherence, and likely burden.

- **RQ1:** *What information obligations and documentation requirements are prescribed by Estonian regulatory information security framework?*
- **RQ2:** *What challenges were identified during the development and implementation of Estonian regulatory information security framework, and how were they addressed?*
- **RQ3:** *What does the overall structure of these obligations reveal about the framework's administrative logic, internal coherence, and likely burden?*

1.3 Research methods

The study primarily employs qualitative document analysis. It examines legal acts, explanatory materials, guidance, and related supporting documents within Estonian regulatory information security framework.

The study uses the Standard Cost Model as a qualitative and analytical point of reference. Its purpose is not to calculate exact compliance costs, but to provide a structured way to describe the administrative implications of information obligations.

Supplementary digital tools were used to support the research and writing process. Search engines and academic databases were used to identify relevant sources and refine search terms for the literature review. Language-support tools were used for proofreading, editing,

and improving general readability. All source selection, classification of obligations, analysis, interpretation, and conclusions remain the author's own.

1.4 Scope and goal

This study focuses on Estonian regulatory information security framework, including the Cybersecurity Act, related regulations, and E-ITS. The analysis is conducted at framework level. It does not attempt to study in depth how individual organisations handle compliance in practice, and it does not measure actual compliance costs. It also does not evaluate whether the framework improves cybersecurity effectiveness.

The expected outcome is a structured analysis of the framework's information obligations, their cumulative architecture, and their likely administrative implications.

1.5 Novelty and contribution

Existing writing on cybersecurity regulation in Estonia has tended to focus on legal obligations, implementation issues, or specific compliance questions. Much less attention has been paid to the framework as a whole from the perspective of information obligations and their administrative implications.

This thesis contributes by examining Estonian regulatory information security framework through its information obligations, documentation requirements, and administrative logic. It offers a structured account of how these obligations are embedded in the framework and how they shape its likely burden and internal coherence.

2. Literature review

A mixed tertiary literature review was conducted on cybersecurity regulation, administrative burden, and compliance-related formalisation. It provides background for interpreting the findings of this thesis.

In this thesis, the literature review serves three functions. First, it shows why cybersecurity regulation can be analysed not only as a legal framework, but also as a source of administrative and documentary obligations. Second, it provides analytical themes for interpreting Estonian framework, especially in relation to information obligations, documentation, burden, coherence, and audit logic. Third, it helps position the thesis within an underexplored field.

2.1 Focus questions for the literature review

The literature review supports the thesis mainly in relation to RQ2 and RQ3. It also provides general background relevant to RQ1. It is not intended to examine Estonian organisations empirically. Instead, it clarifies how earlier literature describes burdens and implementation problems created by regulatory frameworks.

The following focus questions guide the literature review:

- FQ1: How do regulatory frameworks in general affect individual initiative, innovation, and organisational willingness to act or take risks?
- FQ2: What strategies exist in the literature for reducing bureaucratic overhead in regulatory compliance?
- FQ3: How do implementing organisations perceive and navigate the administrative and resource demands associated with cybersecurity framework implementation?

2.2 Literature review protocol

The literature search was conducted using academic databases, digital archives, and supplementary search tools. The main sources used were IEEE Xplore, ScienceDirect, Google Scholar, TalTech Digikogu, and the University of Tartu digital archive ADA. Academic databases and archives were used to identify and access citable literature. Google and ChatGPT were used as supplementary search tools for keyword refinement, source discovery, and reference tracing. These databases, archives, and search tools were selected for their usability and their relevance to cybersecurity, information systems, and regulatory research.

2.3 Synthesis of the literature review

The objective of this literature review is to identify and synthesise academic and practitioner research on regulation, administrative burden, and compliance formalisation. The selected studies were analysed in relation to the literature review focus questions (FQ1–FQ3).

FQ1: How do regulatory frameworks in general affect individual initiative, innovation, and organisational willingness to act or take risks?

At the national or cross-border level, studies have highlighted that excessive or poorly coordinated regulation can distort incentives, discourage entrepreneurship, and hinder economic growth. One analysis [1] points out that uncritical regulatory expansion often shifts costs to the private sector, creates hidden costs on businesses, and limits transparency in policymaking, ultimately suppressing initiative and long-term competitiveness. This aligns with evidence that the quality of regulation itself—rather than its volume—is decisive for innovation: research [2] shows that strong governance and high regulatory quality correlate with greater economic growth and investment, as effective institutions transform regulation into a framework of trust and productive risk taking. Conversely, weak institutional capacity turns the same frameworks into barriers, amplifying administrative inertia. A related cross-border aspect emerges from the export study [3], which reveals

that even when regulation is not directly restrictive, differences in national administrative systems, ICT infrastructures, and public procurement rules can become systemic barriers to collaboration and innovation across borders, particularly in decentralised states like Germany and Belgium.

At the organisational level, the picture is equally complex, though more operational in nature. Small firms and startups face disproportionate administrative demands under ambiguous or fragmented compliance regimes, as evidenced by multiple case studies [4], [5], [6], [7]. Legal uncertainty, lack of state guidance, and limited technical expertise delay product development and discourage engagement with government programmes [4]. The administrative strain emerges less through formal reporting than through resource diversion—such as compliance staffing, IT upgrades, and continuous documentation efforts [6]. Interestingly, many organisations view compliance not primarily as a legal shield but as a reputational necessity [5], suggesting that regulatory trust and legitimacy play as much of a motivational role as enforcement does. Some regulatory frameworks, particularly in cybersecurity, introduce structural contradictions. For instance, the GDPR's implementation has restricted certain data-processing activities vital for threat detection, resulting in a "chilling effect" on proactive security practices [8]. Together, these findings portray a dual dynamic—regulation as both enabler and inhibitor — depending on its design, clarity, and alignment with institutional capacity. National frameworks that promote coherence and transparency foster risk-taking and innovation, while fragmented or overly prescriptive systems increase administrative load and erode initiative at the organisational level [9].

FQ2: What strategies exist in the literature for reducing bureaucratic overhead in regulatory compliance?

At the national level, several studies emphasise the importance of modular, flexible, and context-sensitive regulatory frameworks. For instance, Seeba et al. compare ISO/IEC 27001, CIS Controls, and BSI IT-Grundschutz against Estonian national ISMS requirements and conclude that a BSI IT-Grundschutz-based approach was considered most suitable because it supported national adaptability, free availability, regular updating, levelled controls, and auditability [10]. Similarly, EU-driven reforms and national directives

have led to more structured ISMS, which—when supported by clear templates and harmonised reporting obligations—reduce the interpretive workload for organisations [11]. However, as seen in analyses of frameworks such as E-ITS and ISKE, overly abstract guidance and insufficient readiness among smaller institutions can reintroduce inefficiencies, requiring significant interpretive effort and specialised labour to comply [12][13]. To mitigate this, several authors propose profile-based implementation models, modular audits, and standardised training schemes that scale requirements according to institutional capacity, thereby lowering compliance costs and administrative barriers for low-maturity organisations.

At the organisational level, organisations focus on the use of digital tools and procedural redesign to minimise internal compliance burdens. Process Mining (PM) is presented as one possible method, as it maps real operational data to reveal redundant steps, supports conformance checking, and provides structured, data-driven insights for process improvement [14]. Such data-driven approaches may reduce reliance on manual reporting and subjective interpretation with continuous, automated monitoring, enhancing both transparency and efficiency. Complementary strategies include more explicit role definition, management support, and awareness-building to align compliance with daily operations rather than treating it as an external obligation [15]. The literature also highlights the creation of supportive tools—such as the proposed "E-ITS tool" [13] — to automate documentation, self-assessment, and audit preparation. Such systems directly reduce the human resource intensity of compliance tasks. Together, these studies demonstrate that while regulatory simplification at the policy level is essential, real efficiency gains often depend on digital transformation within organisations. The convergence of modular regulation, automation, and data-driven oversight represents the most consistently supported pathway for reducing bureaucratic overhead in cybersecurity and compliance management.

FQ3: How do implementing organisations perceive and navigate the administrative and resource demands associated with cybersecurity framework implementation?

Empirical evidence suggests that legal ambiguity and a lack of specialised expertise increase compliance costs, particularly for small enterprises that must rely on external consultants or ad hoc interpretations of regulatory guidance [4][5]. Many organisations

struggle to translate broad cybersecurity directives into operational requirements, as frameworks such as E-ITS and ISMS demand continuous documentation, monitoring, and interdepartmental coordination that exceed available capacities [16][17][12]. Even when compliance improves technical controls and staff awareness, as seen after EU-level implementations, these gains are often offset by recurring administrative overhead and limited uptake of advanced measures, such as cryptography, due to resource constraints [11]. Practitioners describe situations where overlapping national and EU requirements produce conflicting obligations and redundant reporting duties, forcing organisations to allocate disproportionate time to procedural documentation rather than to practical risk mitigation [18][19]. The findings indicate that the lack of templates, interpretive guidance, and role clarity creates dependency on vendors or central authorities, reducing internal agility and delaying system updates [12][16]. In relation to framework design, Seeba et al. highlight features such as basic controls, levelled controls, national adaptability, and regular updates as relevant requirements for an Estonian ISMS standard [10]. Overall, the evidence portrays a tension between formal compliance and operational efficiency: while cybersecurity frameworks strengthen governance structures, their complex administrative demands risk undermining initiative, slowing digital transformation, and diverting scarce human and financial resources from core security functions to paperwork and procedural conformity.

2.4 Limitations of the literature review

This literature review is tertiary in nature and primarily synthesises secondary sources. Its analytical depth could be strengthened through closer examination of the primary works cited in the selected studies. Within this thesis, however, its main role is to provide interpretive support for later findings rather than to determine them on its own.

2.5 Research gap

Most academic and policy writing on cybersecurity regulation focuses on legal definitions, compliance obligations, and alignment with EU directives. Much less attention has been

paid to Estonian regulatory information security framework as a whole. Existing studies show that policymakers are advised to assess regulatory impacts [1]. In the case of the Cybersecurity Act, however, the assessment process mainly emphasised expected positive effects and gave limited attention to administrative downsides. Earlier insider-informed work on the development of Estonia's ISMS standard explicitly treated adoption and maintenance costs as relevant design considerations, although primarily from the perspective of national-level standard developers and maintainers [10]. Other work identifies challenges linked to regulatory complexity, administrative demands, and missing automation tools [13]. These concerns were not prominently reflected in the official approval materials [20]. Although some evidence of implementation-related burdens exists [12][16], it remains scattered and limited in scope. There is no structured analysis of the framework's full obligation structure, development issues, and administrative implications.

This thesis addresses that gap through a framework-level analysis of information obligations and their likely burden.

3. Methodology

This chapter presents the methodological approach applied in the thesis. The research is structured around two main analytical areas: the examination of legislative development and regulatory design documents, and the analysis of information obligations embedded in the regulatory framework. Together, these analytical areas support all three research questions by identifying formal obligations, examining the framework's development, and assessing its administrative logic, internal coherence, and likely burden.

3.1 Analysis of legislative development and regulatory design

This section describes the document analysis of legislative development and regulatory design. It defines the sources, scope, and analytical procedure used in chapter 4.

3.1.1 Object and scope of the analysis

The object of analysis is the legislative development of Estonian regulatory information security framework. The analysis focuses on the Cybersecurity Act, its amendments, and related legislative materials. Its scope also includes coordination comments and positions submitted by different stakeholder groups during the legislative process. The analysis examines regulatory intent, scope choices, and burden-related concerns reflected in those documents.

3.1.2 Sources and document selection

The analysis uses legislative and regulatory design documents. These include draft acts, explanatory memoranda, coordination materials, stakeholder comments, committee

materials, and parliamentary records. Documents were selected based on their relevance to the development, justification, contestation, and revision of the framework.

3.1.3 Analytical procedure

The documents were reviewed qualitatively and compared across legislative stages. Attention was given to stated objectives, scope decisions, impact assumptions, and recurring implementation concerns. The analysis traced how these themes developed over time and across amendment cycles.

3.1.4 Methodological limitations

This analysis is limited to what is visible in official documents. It does not show informal negotiations or undocumented decision-making. It therefore supports interpretation of regulatory design, but not a full reconstruction of legislative practice.

3.2 Analysis of information obligations and their administrative implications

This section describes the analysis of information obligations and administrative burden. It defines the analytical framework, scope, and procedure used in chapter 5.

3.2.1 Analytical framework: Tool #58 and its adaptation

This part of the thesis draws on Tool #58, the EU Standard Cost Model, from the European Commission's Better Regulation Toolbox [20]. The tool is used as a qualitative analytical reference, not as a basis for monetary cost calculation. It supports a structured reading of information obligations in the analysed framework.

In this thesis, an information obligation means a regulatory requirement that makes information durable, demonstrable, or transferable. This includes duties to produce or

maintain documents, records, plans, reports, registers, notifications, published information, or similar artefacts. General cybersecurity requirements were excluded unless they required such informational evidence. For example, a technical control was not coded by itself. It was coded only where the text also required a record, document, notification, or other demonstrable output.

The analysis therefore focused on the informational action required by the provision. It did not rely only on the formal wording of the requirement.

3.2.2 Object and scope of the analysis

The object of analysis is the set of information obligations embedded in Estonian regulatory information security framework. The analysis covers the applicable regulatory instruments in force on 15 March 2026. It focuses on obligations arising from the Cybersecurity Act, related regulations, and requirements linked to E-ITS.

3.2.3 Identification and characterisation of information obligations

All applicable regulatory texts were reviewed in full. Identifiable information obligations were recorded in a structured table.

The obligations were identified through manual review rather than keyword search alone. Keyword expressions were tested during the initial coding phase and used as supporting indicators. However, they were not used as the main identification method, because similar information obligations were expressed through varied legal, administrative, and technical formulations. In practice, the same substantive requirement could be described through terms such as documenting, recording, registering, submitting, making available, notifying, approving, or maintaining. For that reason, each provision was read in context and coded according to the substantive informational action it required.

Typical information obligations included documentary, reporting, notification, publication, record-keeping, and availability duties. The analysis recorded the type of obligation created by each provision. The main types included storage, provision, updating, publication,

collection, and availability of information. The analysis also recorded the apparent frequency of each obligation. The main frequency categories were one-off, periodic, and event-based.

The aim was to produce a comprehensive overview of the framework's formal information obligations. This step followed the general logic of Tool #58.

3.2.4 Identification of named documentary requirements

The recorded information obligations were examined for references to specific documentary outputs. The analysis identified whether the obligation referred to a named policy, documented procedure, register, document, plan, or similar artefact. Where such a reference was identifiable, the artefact type and name were recorded.

3.2.5 Validation against official guidance materials

For the analytical cross-check, the identified artefact requirements were compared with official guidance materials. The purpose was to assess whether the named artefacts identified in the regulatory texts corresponded to those presented in implementation guidance.

The validation step was also used as an iterative cross-check of the initial coding. After the first mapping of information obligations had been completed, named documentary artefacts were extracted and compared with the official E-ITS guidance sample-document list. Where the guidance material referred to a documentary requirement that had not previously been coded as such, the regulatory text was reviewed again and the closest corresponding requirement was added to the mapping. This explains why some IO-ID numbers in Appendix 3 contain later inserted sub-identifiers, such as 045-1, while others follow the original sequential numbering. The numbering therefore reflects the development of the coding process and should not be interpreted as a hierarchy of importance.

3.2.6 Methodological limitations

This analysis does not identify the exact set of obligations applicable to any particular organisation. Tool #58 would normally also require identification of the affected entities. That step was not carried out, because the thesis does not analyse specific organisations. The findings should therefore be interpreted as a structural mapping of the framework, not as a full compliance profile for any single organisation. In addition, not all requirements apply uniformly across all regulated entities. The framework itself differentiates between categories of organisations and between different levels of required measures.

The analysis also does not assess cybersecurity effectiveness or whether the framework improves actual security outcomes.

4. Development and regulatory design of the Cybersecurity Act

This chapter analyses the development of Estonian Cybersecurity Act (Küberturvalisuse seadus, KüTS) from its initial conception in 2017 through subsequent amendments in 2021–2022 and 2024–2026. The focus is on regulatory intent, assumptions about scope and administrative implications, and the evolution of administrative and organisational expectations as reflected in legislative documents, explanatory memoranda, and parliamentary discussions. It reconstructs the legislative development of the framework and identifies the main challenges, assumptions, and burden-related concerns visible in the official materials. It thereby establishes the regulatory context for the following chapter's analysis of information obligations, internal coherence, and likely administrative implications.

4.1 Rationale for establishing a unified cybersecurity framework

One of the formal reasons for establishing the Cybersecurity Act was the obligation to transpose Directive (EU) 2016/1148 of the European Parliament and of the Council on the security of network and information systems (NIS Directive) into Estonian law. The deadline for transposition was 9 May 2018 [21].

The legislative process was officially initiated on 17 March 2017 with the submission of the development intent (VTK) by the Ministry of Economic Affairs and Communications [21]. The Cybersecurity Act was adopted on 9 May 2018 and entered into force on 23 May 2018 [22]. Consequently, the period available for preparing, coordinating, and adopting the legislation was slightly over one year.

The development intent identified the existing cybersecurity-related regulation as fragmented across multiple legal acts, with limited coherence between them. It stated that rights and

obligations related to cybersecurity were insufficiently regulated and that supplementing existing sectoral legislation would not enable cybersecurity governance to be regulated to a sufficient extent. On this basis, the preparation of a separate, horizontal legal act was proposed [21].

During the legislative process, references were made to the limited time available before 9 May 2018, and therefore there was no doubt about the need for the rapid preparation and adoption of the draft law [23]. In an opinion submitted on 27 April 2018, when the draft of Cybersecurity Act was already under consideration in the Riigikogu, the Estonian Association of Information Technology and Telecommunications noted that the rapid pace of the parliamentary procedure left limited time for more detailed development of the relevant provisions. [24].

The time constraints of the legislative process were also addressed in parliamentary materials. In its opinion issued in April 2018, the Economic Affairs Committee of the Riigikogu noted that failure to transpose the NIS Directive by the prescribed deadline could result in infringement proceedings being initiated by the European Commission. This consideration was cited in the context of explaining the legislative schedule [25].

In parallel with the transposition requirement, the Cybersecurity Act established a general legal framework for cybersecurity governance in Estonia. The Act defines its subjects, regulates incident handling, sets requirements for addressing vulnerabilities and cyber threats, and establishes supervisory arrangements. It also authorises competent ministers to adopt secondary legislation specifying detailed requirements, including regulations on the cybersecurity of network and information systems, and the application of security measures in the context of cloud services [22].

4.2 Anticipated impacts and administrative burden in legislative design

The development intent document included an initial assessment of the expected impacts of the proposed legislation. It acknowledged that entities which had not previously implemented security measures might require additional resources, potentially including personnel costs and investments in information systems. At the same time, it was argued that

many organisations whose service delivery was already highly dependent on information technology — such as providers of essential services—were already subject to comparable obligations and had therefore planned corresponding resources [21].

The impact assessment did not include a comprehensive evaluation of administrative burden for affected entities, with the exception of the notification obligation related to cybersecurity incidents. The primary quantified administrative impact concerned the Information System Authority (RIA). It was projected that the increase in both the number of supervisory entities and the scope of responsibilities would necessitate the recruitment of additional officials. Overall, the combined assessment characterised the expected impacts as moderate in scope, frequency, and target group size, with a low risk of undesirable effects. On this basis, the preparation of a detailed impact analysis was deemed unnecessary [21].

The development intent estimated that the administrative burden would increase for approximately one hundred entities, primarily due to incident reporting and information request obligations [21]. However, this estimate was challenged during the coordination process. For example, the Ministry of Social Affairs noted that the number of healthcare service providers alone exceeded five hundred, raising questions about the realism of the projected scope [26]. The Ministry of Defence and the Ministry of Justice similarly expressed concerns regarding the adequacy of the impact assessment and the absence of a consolidated view of the law's effects across sectors [23][27].

4.3 Coordination process and contested impact assessments

The draft Cybersecurity Act was submitted for formal inter-ministerial coordination on 3 October 2017. Compared to the development intent, the explanatory memorandum accompanying the draft provided a more detailed description of impacts. Although, these additional details focused predominantly on the perspective of the RIA. The need for five additional positions at RIA was identified, justified by increased supervisory responsibilities, expanded international cooperation, and the analytical workload associated with incident handling [28].

In contrast, the impacts on other regulated entities were described in terms similar to the

development intent. The affected group was characterised as narrow, and the increase in administrative burden was again primarily linked to incident reporting and responses to supervisory inquiries. Cost increases were mainly associated with the implementation of technical and organisational security measures, but no estimates were provided [28].

Several coordinating institutions formally objected to the draft on impact assessment grounds. The Ministry of Social Affairs declined to coordinate the draft, reiterating that the assessment of impacts — particularly in the healthcare sector — was insufficient and that similar concerns had already been raised during the development intent stage [29]. The Ministry of Finance pointed out that the impact on local governments had not been adequately assessed, although potential funding sources were identified [30]. Comparable concerns were raised by the Association of Estonian Cities and the Association of Municipalities of Estonia [31]. The Ministry of Rural Affairs noted that other public authorities beyond those explicitly mentioned might also incur costs, without corresponding descriptions of funding mechanisms [32].

The coordination materials indicate that each institution primarily evaluated the draft from the perspective of its own policy domain, often referring to sector-specific regulatory arrangements already in place. While this is a normal feature of inter-ministerial coordination, it placed increased responsibility on the drafting authority to maintain a comprehensive, state-level perspective. The available documents suggest that such a consolidated view remained limited, as impact assessments continued to focus on specific administrative domains rather than on the cumulative effect of the regulation.

On 13 December 2017, the improved draft was submitted to the Ministry of Justice for coordination [33]. In its response of 14 February 2018, the Ministry of Justice characterised the impact assessment as overly general and provided detailed recommendations for improvement [34]. Although subsequent revisions addressed some of these comments, the revised explanatory memorandum continued to emphasise that the law affected only a limited group of entities and that administrative burden would increase only marginally [35].

4.4 Parliamentary deliberations and scope negotiation

The draft Cybersecurity Act was submitted to the Government on 21 February 2018 [36] and forwarded to the Riigikogu on 5 March 2018 [37]. Parliamentary committee discussions provide further insight into the assumptions underlying the legislation. In the Economic Affairs Committee meeting of 19 March 2018, it was noted that the title "Cybersecurity Act" had been chosen deliberately, as "Network and Information Systems Security Act" was considered too narrow given the intention to expand the regulatory scope in the future. Reference was made to potential future needs to regulate other cybersecurity-related issues, including sectoral coordination and governance arrangements [38].

Despite this acknowledgement of future expansion, discussions continued to frame the immediate impact on businesses as limited. The assessment focused primarily on providers of essential services, and it was emphasised that small enterprises below defined employee and turnover thresholds would be excluded. In discussions, intermediate-sized organisations were not explicitly addressed. The estimate that approximately one hundred entities would be affected was reiterated. The public sector was again described as largely unaffected, on the grounds that state authorities already applied ISKE requirements and would therefore not require additional resources. At the same time, the creation of five new positions at RIA was confirmed to support supervision and cooperation at the European level [38].

During parliamentary deliberations, representatives of industry organisations raised concerns regarding both scope and administrative duplication. The Estonian Association of Information Technology and Telecommunications (ITL) highlighted that although the Act was scheduled to enter into force in May 2018, the identification of regulated service providers by RIA would only be completed several months later. This implied that the actual number of affected entities was not known at the time of adoption. ITL also drew attention to overlapping reporting obligations to multiple supervisory authorities across different sectors, as well as to earlier assessments suggesting a significant increase in administrative burden. Additionally, ITL argued against extending the regulatory scope beyond what was strictly required by the NIS Directive [39].

Readability and interpretability issues were also raised. In April 2018, representatives

of local government organisations noted in parliamentary committee discussions that the Act was difficult to read and understand, particularly for smaller municipalities where responsibility for information and communication technology often rests with specialists who are not legally trained [40].

The Act was ultimately adopted on 9 May 2018 and entered into force on 23 May 2018 [22].

4.5 Amendments and expansion of regulatory scope

4.5.1 First amendment cycle (2021–2022): ISKE to E-ITS

The first significant amendment process began on 1 February 2021. The initial draft proposed replacing the existing ISKE framework with the Estonian Information Security Standard (E-ITS) [41]. As noted by the Ministry of Justice in March 2021, E-ITS was not yet substantively defined in the draft, which led the coordination process to stall [42].

A revised amendment draft was submitted for coordination on 21 September 2021. The explanatory materials explicitly stated that E-ITS would be broader in scope than ISKE. Whereas ISKE applied primarily to information systems, E-ITS was designed to cover the cybersecurity of organisations as a whole. The materials also acknowledged that, in practice, some authorities had avoided applying ISKE by classifying systems in ways that excluded them from the definition of an "information system" under existing law [43].

The amendment expanded the range of entities required to comply with the standard, with the primary emphasis placed on the positive effects for cybersecurity. Potential increases in administrative and organisational burden received comparatively limited attention. The explanatory memorandum argued that increased expenditure on cybersecurity could be offset by the avoidance of costs associated with cyber incidents. It was estimated that, during the implementation phase, personnel responsible for information security would need to devote only several additional hours per week to aligning organisational practices with E-ITS requirements [43].

Although the Ministry of Justice coordinated a revised version of the amendment in early 2022, the detailed content of this version is not visible in the legislative information system [44]. The State Chancellery nevertheless observed that the amendments would increase administrative burden for state authorities, local governments, and regulated enterprises, as organisations would need to address cybersecurity comprehensively rather than focusing solely on systems related to specific services. The explanatory memorandum was criticised for insufficiently assessing these impacts [45].

The amendment was adopted in July 2022 following parliamentary deliberations that were strongly influenced by the broader security situation resulting from the war in Ukraine. During committee discussions, political parties, which were initially included within the scope of the amended Act [46], were later explicitly excluded by politicians [47]. This exclusion illustrates the negotiated nature of regulatory scope definition during the legislative process.

4.5.2 Second amendment cycle (2024–2026): Transposition of NIS2

The second major amendment cycle was initiated to transpose Directive (EU) 2022/2555 (NIS2). Although the directive required transposition by October 2024, the amended Act entered into force on 1 January 2026. The draft amendment was submitted for coordination in December 2024, with the explanatory memorandum identifying the expansion of the list of regulated subjects as the most significant change. At the time, RIA estimated that approximately 3,537 entities were subject to the existing Act, with the number expected to increase to around 5,500 following the amendment [48].

The explanatory memorandum identified major cost drivers for newly regulated entities, including risk assessments and periodic compliance audits [48]. While cost ranges were provided, stakeholders questioned their realism. Coordination feedback from local government associations, the Ministry of the Interior, the Ministry of Finance, and industry organisations consistently highlighted concerns regarding audit capacity, rising audit prices, and the cumulative administrative burden associated with documentation, compliance verification, and ongoing standard maintenance [49][50][51][52].

During parliamentary discussions in autumn 2025, it was acknowledged that the number of

affected organisations could reach several thousand and that there was limited insight into their actual financial and organisational capacity [53]. Readability concerns were again raised, with references to assessments by legal professionals that the draft text was difficult to interpret [54]. Despite these concerns, the amendment was adopted in December 2025 [55].

4.6 Summary: regulatory intent and emerging complexity

Across its initial adoption and later amendments, the Cybersecurity Act reflects a consistent regulatory intent. It aims to strengthen national cybersecurity governance, align with European Union requirements, and establish more uniform standards across sectors.

At the same time, the legislative materials reveal recurring assumptions about impact. Administrative and organisational effects were often expected to remain limited. This remained the case even as the framework expanded. Its scope moved from individual information systems to whole organisations. The number of regulated entities also grew from a relatively narrow group to several thousand.

Concerns about interpretability, documentation workload, audit capacity, and cumulative administrative burden were repeatedly raised. These concerns appeared during both coordination and parliamentary deliberations. They were acknowledged in part, but only limitedly reflected in impact assessments.

Taken together, these findings suggest a recurring tension in the framework's development. Regulatory ambition expanded, while administrative implications were assessed only partially. This pattern provides the context for the next chapter. That chapter examines the framework's layered information obligations. It also considers what that structure suggests about administrative logic, internal coherence, and likely burden.

5. Findings from the analysis of information obligations and documentary requirements

This chapter presents the findings from the analysis of Estonian regulatory information security framework at the level of formal information obligations and documentary requirements. It follows the methodological steps set out in Section 3.2 and proceeds from obligation mapping to document identification and validation against guidance materials. The analysed acts are listed in Appendix 2, which provides the regulatory basis for the findings presented in this chapter.

5.1 Identification and characterisation of information obligations

This section maps the formal information obligations created by the analysed regulatory instruments.

The mapping identified 639 information obligations across the acts listed in Appendix 2 and recorded in Appendix 3. Because the framework is assembled from several sources, not all of these obligations are unique. Some obligations are repeated across legal layers or restated in slightly different forms. Most obligations arise from E-ITS Annex 2, which contains the detailed control catalogue. The framework therefore operates as a layered structure rather than a single consolidated list of duties. The mapped obligations should therefore be read as a framework-level total, not as a compliance set for any single organisation.

The mapped obligations are dominated by storage duties, followed by provision, updating, availability, and publication. Many storage duties concern documents, registers, plans, or records that would also require later updating. The formal wording does not always state this directly, but regular maintenance is often implied. For that reason, periodic burden is likely greater than the frequency labels alone suggest.

The mapping also shows that the regulatory area is wide. The obligations extend beyond narrowly technical controls into governance, operations, applications, infrastructure, networks, continuity, incident handling, industrial environments, and physical facilities. They reach into areas already regulated elsewhere, such as building-related matters and occupational safety. The framework therefore affects organisational arrangements as well as technical safeguards.

The obligation mapping also reveals interpretive strain. In many cases, the text requires something to be documented without clearly specifying the required form. It remains unclear whether a note, ticket, email, record, procedure, or standalone document is expected.

Similar topics are also not documented with equal intensity across comparable modules. For example, Windows Server deployment requires documented selection criteria [IO-ID 442], while the corresponding Linux and Unix module lacks the same wording.

The framework is not always consistent in its terminology for similar documents, which makes interpretation harder. For example, “business continuity” appears as "ärijätkuvus-" in CON.3.M6, but as "talitluspidevus" in SYS.1.1.M22. Likewise, “disaster recovery plan” appears as "toibumisplaan" in OPS.1.1.1.M17, but as "taastekava" in SYS.1.1.M22. While these terms may be semantically correct, such variation makes it harder to determine whether the text refers to the same document or to different ones.

5.2 Identification of named documentary requirements

After mapping information obligations, the analysis identified named documentary requirements within the same regulatory framework. The purpose of this step was to determine which obligations point to a recognisable documentary artefact.

Appendix 4 records 176 entries, of which 164 are unique by name.

The named requirements cover a broad range of document types. These include policies, strategies, concepts, procedures, plans, registers, inventories, records, reports, guidelines, contracts, and rules. The framework therefore prescribes not a single document set, but a wider documentary environment. Not all named artefacts are required from every entity.

Some are relevant only in specific contexts, while others are produced by auditors or other external actors. The resulting documentary environment spans governance, operations, assets, continuity, incidents, procurement, and technical administration. Examples in Appendix 4 include the information security policy, asset register, protection domain description, audit plan, emergency manual, network diagram, and recovery plan. Other named artefacts concern procurement, remote access, outsourcing, data handling, and contractual security arrangements. These findings support the earlier finding that the framework reaches well beyond narrowly technical controls. It also creates documentary expectations in fields already regulated elsewhere.

It is also likely that some of these documentary requirements are compatible with each other and could be combined into a single document. This does not reduce the analytical significance of the finding. Even where documents can be merged, the framework still shows a strong tendency to require formal documentation across many areas.

This step also helps explain why many obligations in the previous subsection were coded as storage duties. In practice, many of those duties concern documents that must be created, kept, and usually updated over time. The formal wording does not always state the update requirement directly. Still, such maintenance is often implied by the purpose of the document itself.

The mapping also shows that documentary requirements are not always named with equal precision. Some obligations refer to a clearly titled artefact, such as a register, plan, or policy. Others only require something to be documented, without identifying the expected document type. This makes it harder to determine whether compliance requires a standalone document, a system entry, or another durable record.

5.3 Validation against official guidance materials

For validation, the identified documentary requirements were compared with the sample-document list used in official guidance materials. The comparison is presented in Appendix 5. Its purpose was to assess whether the artefacts found in regulatory texts also appear in implementation guidance.

The comparison shows overlap, but not one-to-one correspondence. Several central artefacts appear in both sources. These include the information security policy, asset register, and several continuity and management documents. At the same time, the guidance list is much shorter than the list derived from regulatory texts.

The guidance list contains 38 items, while Appendix 4 records 164 unique named artefacts. The official note states that the guidance list is oriented towards medium-sized and larger organisations. It adds that smaller organisations should optimise the list and combine documents. This note is analytically important. If a list intended for medium-sized and larger organisations is already much shorter, the full framework appears highly documentation-intensive.

The comparison also shows that some core guidance documents are not clearly stated as direct requirements in the framework. A clear example is the information security strategy. In Appendix 5, it appears in the guidance list as a core document, but no direct requirement in the regulatory texts can be found.

The same comparison reveals imbalance in document types. The guidance list contains only one clearly labelled concept document. By contrast, the full mapping identified fourteen unique concept documents. This suggests that the guidance material presents a simplified implementation view, not the full documentary structure of the framework.

Naming differences create an additional problem. The same or related artefacts are not always labelled consistently across the guidance and regulatory texts. As a result, the guidance supports implementation, but does not fully resolve questions of naming, scope, or documentary form. This problem is also consistent with the issues noted during the document review.

5.4 Summary: structure, scope, and documentary logic of the framework

The analysis identified a layered framework of 639 information obligations and 164 uniquely named documentary artefacts. These totals describe the framework as a whole. They do

not represent the document set required from any single regulated entity. These obligations are distributed across several legal sources and are concentrated in the detailed E-ITS control catalogue. The framework therefore does not operate through a small set of direct reporting duties alone. It creates a broader documentary environment that organisations must maintain over time.

The findings also show that the framework covers a wide regulatory area. Its obligations extend beyond technical safeguards into governance, continuity, procurement, contractual arrangements, facilities, and other organisational domains. Many documentary requirements can likely be combined in practice. Even so, the framework shows a strong tendency to formalise and document many areas of organisational activity.

The comparison with guidance materials confirms this documentary logic, but not as a stable one-to-one structure. The official sample-document list is shorter and simpler than the document set derived from the regulatory texts. Naming differences, implied requirements, and uneven terminology make the framework harder to interpret consistently.

6. Discussion

This chapter discusses the findings presented in Chapters 4 and 5 in light of the literature reviewed in Chapter 2. Its purpose is to interpret what the framework's structure reveals about regulatory logic, internal coherence, implementability, and likely administrative burden.

6.1 The framework as a documentary compliance regime

One aim of the framework was to reduce fragmentation. The development intent described cybersecurity regulation as dispersed across several acts and lacking coherence. A separate horizontal framework was therefore proposed.

This objective is broadly consistent with the literature reviewed in Chapter 2. The review suggests that coherent and transparent frameworks can reduce uncertainty. It also suggests that modular and context-sensitive designs can lower interpretive and administrative burden [9, 10]. RIA presents E-ITS in similar terms. It describes E-ITS as an Estonian-language basis for information security management, aligned with ISO/IEC 27001 and adapted to the national legal context [56].

From this perspective, E-ITS and the wider framework can be read as an attempt to make a fragmented regulatory area more governable. The solution, however, was not only legal consolidation. It was also documentary formalisation. Chapter 5 identified 639 information obligations and 164 uniquely named documentary artefacts. These are distributed across several legal layers and are concentrated in the detailed E-ITS control catalogue.

The framework therefore does not operate mainly through a small number of direct reporting duties to the state. Instead, it requires organisations to maintain internal documentation

that can be reviewed, updated, and demonstrated when needed. This includes policies, procedures, plans, registers, inventories, records, descriptions, and other formal artefacts. The framework governs not only what organisations must do, but also how that activity must be rendered visible in documented form.

In that sense, the framework can be described as a documentary compliance regime. Its central governance technique is not direct control of every technical act. It is the requirement that organisations define, record, retain, and present the structures through which security is managed. Documents do not merely support compliance. They become one of its principal objects and instruments.

This does not make documentation unnecessary or irrational. Some documentary requirements have clear governance value. Policies can allocate responsibility. Registers can support oversight. Plans can structure continuity and incident response. Documented decisions can preserve organisational memory and support accountability. In a resilience-oriented field, some documentary formalisation is therefore expected.

At the same time, the findings suggest that the framework gives documentary form a particularly central role. Many obligations are framed as storage, updating, availability, or provision duties. Many named artefacts concern governance, continuity, procurement, contracts, facilities, and other domains beyond narrow technical controls. The framework therefore treats security as something that must be made formally legible across the organisation, not only technically implemented.

This finding can also be read through institutional and audit-oriented theories of organisations. Formal structures do not only serve technical coordination; they may also demonstrate legitimacy, responsibility, and control [57]. In audit-oriented governance, procedures and documentary traces become important because they make organisational activity visible and verifiable [58]. Similarly, where the connection between formal measures and operational outcomes is difficult to observe, organisations may still expand compliance structures as recognised signs of proper management [59]. From this perspective, documentation in the framework functions both as an operational tool and as evidence that security governance exists.

This is important for the present analysis. Documentation serves different purposes. Some

documents support day-to-day work; others preserve traceability, allocate responsibility, or support review. Some mainly exist because auditors, supervisors, or other external actors expect them. A framework with many documentary obligations therefore does more than create paperwork: it shapes what counts as acceptable proof of good security governance.

The comparison with guidance materials supports this interpretation. The official sample-document list is shorter and simpler than the document set derived from the regulatory texts. This suggests that the implementation view presented to organisations is more compact than the formal structure of the framework itself. Even so, the underlying regulatory logic remains documentary. Compliance is organised through artefacts that must exist, be maintained, and be available as evidence.

For the purposes of this thesis, the main point is analytical. The framework should not be understood only as a catalogue of security controls. It should also be understood as a regime that governs through documentation. This does not yet show that the framework is disproportionate. It does, however, establish the basis for the following sections. If compliance is structured through documentary artefacts, then questions of clarity, implementability, and cumulative burden become central rather than secondary.

6.2 Clarity, coherence, and interpretive burden

The burden of the framework is not only documentary. It is also interpretive. A substantial part of compliance effort lies in determining what is required, in what form, and at what level of detail. The literature reviewed in Chapter 2 supports this reading. Clear templates and harmonised obligations can reduce interpretive workload. Abstract guidance and missing templates can increase dependence on external expertise.

The legislative materials indicate that these concerns were visible early in the process. Readability and interpretability were raised in both coordination and parliamentary discussions. Local government representatives noted that the Act was difficult to read and understand, especially for specialists without legal training. Similar concerns reappeared during the later amendment cycle, when legal professionals again described the draft text as difficult to interpret. As the framework expanded from systems to organisations, questions

of scope and application became harder to resolve.

The findings in Chapter 5 help explain why these concerns persisted. The framework is layered across several legal sources, and some obligations are repeated or restated across those layers. Comparable domains do not always show the same documentary intensity. For example, the Windows Server module requires documented selection criteria, while the comparable Linux and Unix module does not. This does not by itself make one rule incorrect. It does, however, make the logic of documentation harder to follow.

The same problem appears in documentary form and terminology. Some obligations refer to clearly named artefacts, such as a register, plan, or policy. Others require only that something be documented, without specifying the expected form. It may be unclear whether a standalone document, a ticket, a system entry, or another durable record is sufficient. Terminology also varies across the framework. Similar continuity and recovery documents appear under different Estonian terms in different modules. Such variation may be linguistically defensible, but it still increases interpretive effort.

A related issue concerns the textual character of E-ITS itself. The standard is largely adapted from the BSI tradition and rendered into Estonian legal and administrative language. That background is not problematic in itself. However, where translation, adaptation, and later revision are not supported by stable terminology and consistent editorial control, different drafting layers remain visible in the text. This matters analytically because a complex technical standard can still be usable if its conceptual vocabulary is stable. By contrast, even justified requirements become harder to implement when the language of the framework introduces avoidable ambiguity.

The framework also contains signs of cross-referencing and alignment problems. These include possible overlap between "DER.3 Infoturbe hindamine" and the audit rules in Cybersecurity Act Annex 3, as well as references that appear to reflect earlier versions of the legal framework. When obligations and audit expectations are spread across several texts, even minor inconsistencies can have disproportionate effects. They increase the effort needed to reconstruct the applicable rule and weaken confidence that the framework can be followed without external interpretive support.

The comparison with guidance materials reinforces this point. The sample-document list is

much shorter than the document set derived from the regulatory texts, and the overlap is not one-to-one. Some guidance documents are presented as important for implementation even where their status as direct requirements is not fully clear from the framework itself. Naming differences also remain unresolved. Guidance therefore supports implementation, but does not fully stabilise the documentary structure.

Taken together, these findings suggest that internal coherence is only partial. The framework does not merely require organisations to comply. It also requires them to reconstruct the meaning of compliance from several layers of text. This creates interpretive burden in addition to documentary burden. It also makes implementation more dependent on auditors, consultants, and informal practice. In that sense, clarity and coherence are not secondary drafting issues. They are part of the framework's practical regulatory impact.

6.3 Proportionality, capacity, and implementability

Proportionality is not only a question of whether security requirements are justified. It is also a question of whether they can be implemented, as prescribed, across organisations with different starting conditions.

This issue is especially important in the present framework. Compliance does not depend only on technical controls. It also depends on organisational capacity. Chapter 2 suggests that this capacity is unevenly distributed. Smaller organisations and those with lower institutional maturity face stronger strain where compliance requires continuous documentation, interdepartmental coordination, and specialised expertise. The same literature suggests that legal ambiguity and weak guidance increase reliance on consultants, vendors, and other external support. By contrast, modular approaches and clearer implementation models can make compliance more manageable for organisations with fewer resources.

The legislative materials indicate that proportionality was only partly addressed in design. Administrative and organisational effects were repeatedly expected to remain limited. This assumption remained visible even as the framework expanded from systems to organisations and from a narrow group to several thousand entities. During the later amendment cycle, it

was expressly acknowledged that there was only limited insight into the actual financial and organisational capacity of the affected organisations. At the same time, stakeholders raised concerns about audit capacity, rising audit prices, and the burden of ongoing documentation and standard maintenance.

The findings in Chapter 5 help explain why this matters in practice. The framework reaches beyond narrowly technical safeguards into governance, continuity, procurement, contractual arrangements, facilities, and other organisational domains. Many obligations concern documents, registers, plans, and records that must not only exist, but also be maintained over time. Implementation therefore presupposes more than technical competence. It also presupposes stable internal roles, routines, and administrative discipline.

This difference is likely to matter at organisational level. An entity with established management structures, dedicated security staff, and mature internal processes can absorb these requirements more easily. A smaller or less formalised organisation may need to create those structures while also meeting the substantive requirements. In such settings, the same framework can generate a very different implementation challenge even before any question of effectiveness is considered.

The point is not that smaller organisations should be exempt from cybersecurity requirements. The point is that the practical meaning of the same requirement changes with organisational capacity. A documented role structure, continuity arrangement, or supplier control process may be routine in one organisation and institution-building in another. From that perspective, proportionality depends not only on the wording of the rule, but also on the assumptions it makes about the organisation expected to apply it.

This also helps explain why breadth matters as much as quantity. A framework may contain many obligations and still remain manageable if those obligations fit existing organisational structures. The present framework, however, often presumes that such structures already exist. Where they do not, implementation requires not only compliance activity, but the building of formal structures needed for compliance.

At the same time, this thesis does not map the exact obligation set for each type of regulated entity. The analysis is conducted at framework level and does not produce a full compliance profile for any individual organisation. For that reason, it cannot determine which entities

face disproportionate burden in practice. It can, however, show that the framework contains several features that the literature associates with uneven implementability: broad organisational reach, ongoing documentation, and dependence on specialised coordination and support.

Taken together, these findings suggest that proportionality in Estonian regulatory information security framework cannot be assessed only at the level of formal legal scope. It must also be assessed at the level of organisational capacity. The framework appears to assume a degree of administrative maturity that will not be present equally across all regulated entities. This does not make the requirements unjustified. It does mean that their practical implementability is likely to vary substantially across differently sized and differently prepared organisations.

6.4 Regulatory expansion and cumulative burden

The previous sections examined the framework as documentary, interpretive, and capacity-dependent. A further issue is how burden accumulates over time. The problem is not only that the framework is broad in its current form. It is also that it has expanded through successive legislative and regulatory additions.

Chapter 4 shows this development clearly. The initial Cybersecurity Act created a horizontal framework for cybersecurity governance. The later ISKE-to-E-ITS amendment broadened the focus from information systems to organisations as a whole. The NIS2 transposition then extended the scope further, increasing the number of regulated entities from an estimated 3,537 to around 5,500.

At the same time, the legislative materials show recurring concern about burden. During coordination and parliamentary debate, stakeholders repeatedly raised questions about documentation workload, audit capacity, rising audit prices, and the cumulative organisational effort associated with maintaining compliance. These concerns were acknowledged, but only partly reflected in formal impact assessments. Chapter 4 therefore suggests a repeated pattern: regulatory scope expanded, while negative and cumulative effects remained only partially assessed.

This pattern matters because cumulative burden does not arise only from the number of duties. It also arises from how they are distributed and maintained. Chapter 5 showed that some obligations are repeated or restated across legal layers. Others are embedded in different instruments that must be read together. In that kind of structure, organisations do not encounter burden only as single tasks. They encounter it as a continuing obligation to maintain, align, and demonstrate compliance across an expanding regulatory whole.

A technically detailed framework that is fixed through formal legal instruments may adapt more slowly than the environment it regulates. The continued presence of the Windows Server 2012 module after end-of-life illustrates this concern. Even where limitations are noted in the text, the continued inclusion of outdated material can weaken trust in the framework and add to interpretive confusion. This raises a broader question about the sustainability of embedding rapidly changing technical expectations in ministerial regulation and standard catalogues that are slower to revise.

Seen in this way, regulatory expansion has effects beyond formal scope. Each amendment may be defensible in isolation. A broader organisational standard may improve coverage. NIS2 transposition may be legally necessary. More detailed controls may strengthen consistency. Yet when requirements are added faster than they are simplified, harmonised, or removed, the framework becomes more burdensome as a whole.

This is also why framework-level analysis matters. Looking only at individual measures risks understating the administrative effect of the whole. Many single obligations can appear reasonable when read separately. The cumulative burden emerges when these obligations are combined, maintained over time, and linked to audit and verification processes. In that sense, the burden is systemic rather than incidental.

The findings therefore support a more structural interpretation of burden. Administrative pressure is produced not only by documentary intensity, interpretive difficulty, or uneven organisational capacity. It is also produced by regulatory accumulation over time. The framework has expanded through addition more than through simplification. The discussion therefore suggests that its burden is best understood not as a problem of single excessive duties, but as the combined effect of documentary formalisation, interpretive complexity, uneven implementability, and cumulative regulatory growth.

7. Recommendations for improvement

The main purpose of this thesis is analytical. It describes the structure of Estonian regulatory information security framework, examines the challenges visible in its development, and interprets the framework's likely administrative implications at framework level. Even so, the findings also support several practical recommendations. These do not point towards the replacement of the existing framework with an entirely new one. Rather, they suggest that the present framework would benefit from clarification, consolidation, and more precise implementation support.

7.1 Recommendation 1: Avoidance of a new parallel framework

The first recommendation is that **simplification should not take the form of creating a wholly new standard**. From the perspective of implementation burden, one of the most disruptive outcomes would be the introduction of another full framework. That would require organisations to repeat earlier work in a new conceptual structure, including interpretation, internal translation, staff training, and documentary redesign. The same concern applies to the idea of introducing an additional layer of measures between the current initial security measures and the E-ITS control catalogue. Such a structure would likely make the framework more fragmented rather than more understandable. If organisations had to navigate initial measures, intermediate measures, and the E-ITS catalogue in parallel, the result would likely be another interpretive layer rather than a clearer compliance path.

7.2 Recommendation 2: Harmonisation of terminology and reduction of avoidable duplication

A more realistic direction would be to improve coherence within the existing framework. One part of this is **vocabulary harmonisation**. The analysis showed that similar requirements and documentary artefacts are not always named consistently across the framework. Such variation creates interpretive burden because it becomes harder to determine whether different terms refer to the same document, to related documents, or to substantively different requirements. A more consistent vocabulary would therefore improve readability, training, implementation, and auditability without changing the underlying security logic.

The second part of internal consolidation would be the **treatment of duplicative requirements**. Duplication should be understood here in a broad sense. It includes not only requirements that are repeated within E-ITS or across different legal layers, but also requirements whose substance is already regulated elsewhere. In such situations, the issue is not necessarily that the requirement itself is unjustified. The issue is that organisations may be required to demonstrate materially similar arrangements several times, under different labels, formats, or control structures. Where requirements substantially overlap, the framework should more clearly indicate whether one documented arrangement satisfies several obligations at once. This would help reduce avoidable duplication without weakening security expectations.

7.3 Recommendation 3: Clarification of documentary expectations

A particularly useful improvement would therefore be a clearer **documentary map linked directly to the applicable requirements**. Such a tool or annex should indicate which documents, records, procedures, plans, registers, or other durable outputs are expected. Each artefact should be linked to the corresponding requirement. It should also indicate whether several obligations may be satisfied through one combined artefact. It should also use the same terminology as the regulatory text itself. The analysis in this thesis showed that naming differences and implied documentary requirements are among the reasons why

the framework is difficult to interpret consistently. A documentary map would therefore not be a secondary convenience, but a practical clarification instrument.

The same applies to sample documents. Especially for requirements that apply broadly across regulated entities, **illustrative examples** would help clarify the expected level of abstraction. In many cases, the practical difficulty is not understanding that something must be documented, but understanding what counts as sufficient documentation. A sample document can show whether the expected output is a short internal rule, a structured procedure, a policy-level text, a register entry, or another form of evidence. The purpose of such samples would not be to impose rigid templates, but to reduce ambiguity and improve proportionality in implementation.

7.4 Recommendation 4: Improvement of implementation tools and scaling support

The need for a **clearer implementation support tool** is also visible in the existing E-ITS tool. The tool already performs a useful function by helping organisations select measures and prepare an implementation plan. However, even a sample organisation with minimal assumptions, no selected organisational or technical practices, and no identified impact from base threats may still receive a very large measure set. This suggests that the tool does not yet reduce complexity to a level that would clearly support low-maturity or smaller organisations. Conversely, the option to display only the "most important measures" may reduce the visible number of measures sharply, but its legal and practical meaning remains unclear. If that option reflects only prioritisation, then the tool should say so explicitly. If it implies that some measures are optional or secondary in a compliance sense, then that would require a much clearer normative basis. Otherwise, the tool risks creating uncertainty about whether organisations are seeing a phased implementation sequence or an actual applicability threshold.

For that reason, implementation aids should be developed further in a way that is more transparent about legal status, applicability, and documentary consequences. Organisations need not only a filtered list of measures, but also a clearer explanation of which requirements

are mandatory for them, which can be implemented later as part of a maturity path, and which documentary outputs are expected as evidence of compliance. In the present framework, this distinction is often difficult to reconstruct from the legal texts alone.

A further recommendation concerns scaling. The findings of this thesis suggest that one source of burden lies in the need to reconstruct applicability from a complex legal structure. A more useful support mechanism would be a **scaling tool**. It would use the organisation's legal status and general characteristics. On that basis, it would show which requirements are likely to apply. It would also show which documentary outputs those requirements imply. In addition, it could show where documents can be combined across domains. Such a tool would be more helpful than a simple reduction in the number of visible measures. It would address the deeper problem of interpretive burden. The aim should therefore not be only to show fewer measures. It should also be to show more clearly why particular measures apply and how they can be satisfied in a manageable way.

7.5 Recommendation 5: Establishment of a more flexible maintenance model

The framework would also benefit from a more **flexible maintenance model**. At present, detailed requirements are embedded in legal instruments that may be slow to amend. This is problematic even when the issue is only inconsistent wording, outdated terminology, or obvious editorial misalignment. In a field as dynamic as information security, that can weaken both clarity and credibility over time. It is therefore worth considering a more agile maintenance model for the detailed catalogue and related implementation materials. Such a model should still preserve the necessary legal basis and oversight. One possible solution would be to give RIA clearer powers within a legally defined framework. These powers could cover controlled clarifications, editorial corrections, and more regular implementation specifications.

7.6 Recommended direction of improvement

Taken together, these recommendations point towards a specific kind of reform. The analysis does not suggest that the main problem is the absence of security requirements. Nor does it suggest that the best response would be a new parallel framework. The more immediate need is for internal consolidation, clearer terminology, better recognition of overlap, more transparent scaling, and stronger implementation aids. In that sense, the framework would benefit less from expansion than from clarification. Its documentary character would remain. However, it could become more coherent, more predictable, and more manageable in practice.

In institutional terms, these improvements require a distinction between formal legal maintenance and practical implementation support. Many requirements are embedded in legal acts or ministerial regulations. Therefore, terminology harmonisation, reduction of duplication, and changes to the maintenance model require formal regulatory action, not ordinary guidance updates. RIA could provide technical and practical input. It could also improve areas that fall within implementation support, such as guidance materials, sample documents, tools, and explanatory materials. Auditors and implementing organisations should also be involved as consultation partners. They are directly exposed to interpretive and evidentiary problems in practice.

8. Conclusion

This thesis examined Estonian regulatory information security framework through the information obligations it prescribes. It asked what obligations the framework creates, what problems appeared during its development, and what its structure reveals about burden and coherence. The analysis was conducted at framework level, using legal acts, explanatory materials, guidance, and related sources. It did not measure the exact burden of any single organisation. Its purpose was to make the framework's administrative structure visible.

The findings show that the framework is broad, layered, and strongly documentary in character. The mapping identified 639 information obligations and 164 uniquely named documentary artefacts. These totals describe the framework as a whole, not the compliance profile of one entity. Even so, they show that the framework operates through much more than direct reporting duties. It creates a wider environment of policies, plans, registers, procedures, records, and audit materials. These must be created, maintained, interpreted, and demonstrated over time.

The analysis of legislative development showed a recurring tension between regulatory ambition and limited burden assessment. The framework expanded from a narrower system-focused model towards a broader organisational model. At the same time, concerns about readability, documentation workload, audit capacity, and cumulative burden were repeatedly raised. These concerns appeared in both coordination and parliamentary discussion. Yet they were only partly reflected in the impact assessments. The development history therefore supports the view that implementability problems were visible early and remained visible later.

Taken together, these findings support the conclusion that the framework functions as a documentary compliance regime. Its main technique is not direct supervision of every technical act. Instead, it requires organisations to make security visible in durable and

reviewable form. In that sense, documents are not only aids to compliance. They are also one of its main objects. This does not make documentation unnecessary. Many documentary requirements may support accountability, continuity, and traceability. Still, the framework gives documentary form a particularly central role.

The study also suggests that the framework assumes managerial attention, administrative capacity, and organisational stability that cannot be expected equally across regulated entities. Organisations do not pursue cybersecurity in isolation. They balance it against continuity, cost control, legal exposure, and core business demands. In the Estonian context, where specialised cybersecurity and compliance capacity is limited, this issue may be sharper. Extensive compliance work may redirect scarce expert capacity from operational security tasks towards documentation and demonstrable conformity. Compliance is therefore shaped not only by security goals, but also by competing organisational priorities.

For that reason, the burden identified in this thesis should not be read in isolation from the wider compliance environment. Cybersecurity obligations do not arrive in an empty organisational space. They compete with other legal, administrative, and operational demands for limited time, expertise, and managerial attention. A requirement that appears manageable in isolation may become burdensome when added to many others. The problem is therefore cumulative rather than measure-specific.

The findings also show that burden is not only documentary. It is also interpretive. The framework is spread across several legal layers. Similar obligations are not always named consistently. Some requirements imply documentation without clearly identifying the required form. This increases the effort needed to determine what must exist, what can be combined, and what counts as sufficient evidence. In practice, this may increase reliance on auditors, consultants, and informal interpretation. Clarity and coherence therefore matter as part of the framework's burden, not as secondary drafting issues.

A further conclusion concerns organisational fit. Many individual measures can be justified when viewed separately. The more difficult question is whether the package remains workable across differently structured organisations. This is especially relevant where the framework reaches beyond narrow technical controls. It extends into governance, personnel, procurement, facilities, continuity, and contractual arrangements. In organisations whose

core activity is not information technology, this may be experienced as an added governance layer. The compliance task then includes organisational translation work, not only security work.

This thesis does not show that all documentary requirements are excessive. Nor does it establish exact compliance costs for particular sectors. It does, however, show that Estonian regulatory information security framework has a cumulative administrative structure that deserves analysis on its own terms. The main burden appears to arise from four connected features. These are documentary formalisation, interpretive complexity, uneven organisational capacity, and regulatory accumulation over time. Taken together, these features help explain why a framework of individually plausible measures may still become difficult to absorb in practice.

The main contribution of this thesis is analytical. It shows that Estonian regulatory information security framework should be understood not only as a legal or technical system, but also as an administrative structure built through information obligations. From that perspective, questions of clarity, organisational fit, and cumulative burden become central.

These findings also have practical implications for framework development. As discussed in Chapter 7, they support efforts to improve terminological coherence, reduce duplication, clarify documentary expectations, and strengthen implementation support.

Further research could examine organisation-specific compliance profiles, sectoral variation, and the relationship between documentary requirements and technical alternatives such as logs, tickets, and system evidence. This would help clarify when documentation supports security practice, and when it mainly supports demonstrable compliance.

References

[1] OECD. *Assessing the Impacts of Proposed Laws and Regulations*. Paris, 1997. DOI: 10.1787/5kml6g5bc1s6-en.

[2] Hossein Jalilian, Colin Kirkpatrick, and David Parker. „Creating the Conditions for International Business Expansion: The Impact of Regulation on Economic Growth in Developing Countries - A Cross-Country Analysis“. In: (Feb. 2003).

[3] Eike Maria Vatsar. „Eesti avaliku sektori e-lahenduste ekspordi takistused“. Master's thesis. Tallinn University of Technology (TalTech), School of Business and Governance, 2021. URL: https://digikogu.taltech.ee/et/Item/f8350b9f-5add-4a4b-a2bc-e16c59e5428c.

[4] Ebru Shentyurk. „Data Protection Regulations Effect on Startups: GovTech Ecosystem in Lithuania“. Master's thesis. Tallinn University of Technology (TalTech), School of Information Technology, 2023. URL: https://digikogu.taltech.ee/et/Item/aca23ea7-611b-4657-9e2d-de64e0fdf03a.

[5] Grete Õigemeel. „Isikuandmete kaitse üldmäärusega kaasnevad väljakutsed ja mõjud väikeettevõtete rakenduskoormusele: Eesti turundus- ja reklaamivaldkonna ettevõtete kaasus“. Master's thesis. Tallinn University of Technology (TalTech), School of Business and Governance, 2018. URL: https://digikogu.taltech.ee/et/Item/809bc66b-ade1-4bc5-87af-bf23bdc82c98.

[6] Kristina Mjasojedova. „Regulatsioonide mõju tarbimislaenude turule aastatel 2011-2021 OÜ Omaraha näitel“. Bachelor's thesis. Tallinn University of Technology (TalTech), School of Business and Governance, 2021. URL: https://digikogu.taltech.ee/et/Item/8a30963d-9107-455c-8be7-2e71a92112ef.

[7] Tarlan Omarbayli. „To have or not to have a GovTech lab? A comparative study of Estonia and Lithuania's models to foster GovTech“. Master's thesis. Tallinn University of Technology (TalTech), School of Business and Governance, 2025. URL: https://digikogu.taltech.ee/et/Item/b0b9fba1-a5d8-48b9-a57c-06bb28622c16.

[8] Marta Terletska. „Reconciling Privacy and Cybersecurity in the European Union Post-GDPR“. Master's thesis. Tallinn University of Technology (TalTech), School of Business and Governance, 2024. URL: https://digikogu.taltech.ee/et/Item/2d437ee2-9da9-4b87-8e5c-87e6676fe223.

[9] Efecan Yildiz. „Impact of Motivation on Employee Performance at a Bank in Estonia“. Master's thesis. Tallinn University of Technology (TalTech), School of Business and Governance, 2020. URL: https://digikogu.taltech.ee/et/Item/3921d146-7fa4-45f0-9bfb-d6fb834362d8.

[10] Mari Seeba, Raimundas Matulevičius, and Ilmar Toom. „Development of the Information Security Management System Standard for Public Sector Organisations in Estonia“. In: *Business Information Systems* 1 (2021), pp. 355–366. DOI: 10.52825/bis.v1i.43. URL: https://www.tib-op.org/ojs/index.php/bis/article/view/43.

[11] Edyta Karolina Szczepaniuk et al. „Information security assessment in public administration“. In: *Computers & Security* 90 (2020), p. 101709. DOI: 10.1016/j.cose.2019.101709. URL: https://www.sciencedirect.com/science/article/pii/S0167404819302469.

[12] Marika Rand. „Estonian Information Security Standard Implementation Challenges Based on One Public Sector Organization“. Bachelor's thesis. Tallinn University of Technology (TalTech), School of Information Technologies, 2025. URL: https://digikogu.taltech.ee/et/Item/a914eda1-0bfe-4cde-82c5-3e9391976308.

[13] Anto Veldre. „Eesti infoturbestandardi protsessimudeli evalveerimine“. Diploma thesis. Tallinn University of Technology (TalTech), School of Information Technologies, 2021. URL: https://digikogu.taltech.ee/et/Item/1e4a4d90-e66e-4ef8-ae01-11b311cd7e02.

[14] Jonathan Grundmann. „Decoding bureaucracy: towards a process mining method for public administration“. Master's thesis. Tallinn University of Technology (TalTech), School of Business and Governance, 2025. URL: https://digikogu.taltech.ee/et/Item/210635d0-44fd-4851-bf50-9eaa7384c123.

[15] Liisbeth Laasik. „Data Governance in the Estonian Government Sector: The Motives and Strategies for Implementation“. Master's thesis. Tallinn University of Technology (TalTech), School of Information Technology, 2023. URL: https://digikogu.taltech.ee/et/Item/760fcd57-4c8e-4b37-be76-5f742dd069ab.

[16] Kadri Koit. „Eesti infoturbe standardi (E-ITS) nõuete kirjeldamine riigihangetes“. Master's thesis. University of Tartu, Institute of Computer Science, 2024. URL: https://hdl.handle.net/10062/104992.

[17] Elen Kivi. „Dokumentatsioon IT süsteemis“. Master's thesis. University of Tartu, Institute of Computer Science, 2011. URL: http://hdl.handle.net/10062/33034.

[18] Enrriko Kapiti. „What role conflict do ICT professionals in government experience while implementing ICT projects? The case of Belgium“. Master's thesis. Tallinn University of Technology (TalTech), School of Business and Governance, 2025. URL: https://digikogu.taltech.ee/et/Item/b28114a8-dd4a-4230-83b3-ef2f4c31dda0.

[19] Ele-Merike Pärtel. „Eesti riikliku andmete teabevärava lahenduse kavandamine“. Master's thesis. Tallinn University of Technology (TalTech), School of Information Technologies, 2025. URL: https://digikogu.taltech.ee/et/Item/97937da3-bacf-4d90-bcca-17d5ccf2d3a5.

[20] European Commission. *Better Regulation Toolbox: Chapter 8 – Methodologies for Analysing Impacts in Impact Assessments, Evaluations, and Fitness Checks*. European Commission. 2025. URL: https://commission.europa.eu/document/download/0d32ee11-92da-434d-9c86-fd4579d95dc6_en?filename=BR%20Toolbox%20-%20Dec%202025%20-%20Chapter%208.pdf.

[21] Majandus- ja Kommunikatsiooniministeerium. *Kübervaldkonna seaduse väljatöötamiskavatsus*. EIS document no. 17-0361/01 (17.03.2017). URL: https://eelnoud.valitsus.ee/main/mount/docList/0cb6f664-ad24-42e2-aa06-0a816484f79b.

[22] Riigikogu. *Küberturvalisuse seadus*. no 252, adopted 09.05.2018, entered into force 23.05.2018. Riigi Teataja. URL: https://www.riigiteataja.ee/en/eli/523052018003/consolide.

[23] Kaitseministeerium. *Väljatöötamiskavatsuse kooskõlastamine*. EIS document no. 17-0361/04 (02.05.2017). URL: https://eelnoud.valitsus.ee/main/mount/docList/0cb6f664-ad24-42e2-aa06-0a816484f79b.

[24] Eesti Infotehnoloogia ja Telekommunikatsiooni Liit. *Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu (ITL) täiendav arvamus küberturvalisuse seaduse eelnõu 597 SE kohta*. E-mail to the Riigikogu National Defence Committee, 27.04.2018. Registered in Riigikogu legislative file 597 SE. URL: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/.

[25] Riigikogu majanduskomisjon. *Riigikogu majanduskomisjoni arvamus küberturvalisuse seaduse eelnõu 597 SE kohta*. Opinion to the Riigikogu National Defence Committee, 03.04.2018. Registered in Riigikogu legislative file 597 SE. URL: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/.

[26] Sotsiaalministeerium. *Kübervaldkonna seaduse väljatöötamise kavatsuse kooskõlastamine*. EIS document no. 17-0361/03 (26.04.2017). URL: https://eelnoud.valitsus.ee/main/mount/docList/0cb6f664-ad24-42e2-aa06-0a816484f79b.

[27] Justiitsministeerium. *Kübervaldkonna seaduse väljatöötamise kavatsuse kooskõlastamine*. EIS document no. 17-0361/06 (29.05.2017). URL: https://eelnoud.valitsus.ee/main/mount/docList/0cb6f664-ad24-42e2-aa06-0a816484f79b.

[28] Majandus- ja Kommunikatsiooniministeerium. *Küberturvalisuse seaduse eelnõu kooskõlastamine, Annex 2: Küberturvalisuse seaduse eelnõu seletuskiri*. EIS document no. 17-1085/02 (03.10.2017). URL: https://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b.

[29] Sotsiaalministeerium. *Küberturvalisuse seaduse eelnõu kooskõlastamine*. EIS document no. 17-1085/09 (02.11.2017). URL: https://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b.

[30] Rahandusministeerium. *Küberturvalisuse seaduse kooskõlastamine*. EIS document no. 17-1085/10 (03.11.2017). URL: https://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b.

[31] Eesti Maaomavalitsuste Liit and Eesti Linnade Liit. *Küberturvalisuse seaduse eelnõu kooskõlastamine*. EIS document no. 17-1085/06 (03.11.2017). URL: https://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b.

[32] Maaeluministeerium. *Seaduseelnõu kooskõlastamine*. EIS document no. 17-1085/03 (19.10.2017). URL: https://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b.

[33] Majandus- ja Kommunikatsiooniministeerium. *Küberturvalisuse seaduse eelnõu kooskõlastamine*. EIS document no. 17-1085/13 (13.12.2017). URL: https://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b.

[34] Justiitsministeerium. *Küberturvalisuse seaduse kooskõlastamine*. EIS document no. 17-1085/15 (14.02.2018). URL: https://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b.

[35] Vabariigi Valitsus. *Seaduseelnõu algatamine, Annex 2: Seletuskiri*. From Vabariigi Valitsus to Riigikogu, EIS document no. 17-1085/18 (01.03.2018). URL: https://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b.

[36] Majandus- ja Kommunikatsiooniministeerium. *Küberturvalisuse seadus*. EIS document no. 17-1085/16 (21.02.2018). URL: https://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b.

[37] Vabariigi Valitsus. *Seaduseelnõu algatamine*. From Vabariigi Valitsus to Riigikogu, EIS document no. 17-1085/18 (01.03.2018). URL: https://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b.

[38] Riigikogu majanduskomisjon. *Riigikogu majanduskomisjoni istungi protokoll nr 195 (19.03.2018)*. Registered in Riigikogu legislative file 597 SE. URL: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/.

[39] Eesti Infotehnoloogia ja Telekommunikatsiooni Liit. *Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu (ITL) arvamus küberturvalisuse seaduse eelnõu 597 SE kohta*. E-mail to the Riigikogu National Defence Committee, 29.03.2018. Registered in Riigikogu legislative file 597 SE. URL: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/.

[40] Riigikogu riigikaitsekomisjon. *Riigikogu riigikaitsekomisjoni istungi protokoll nr 231 (09.04.2018)*. Registered in Riigikogu legislative file 597 SE. URL: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/.

[41] Majandus- ja Kommunikatsiooniministeerium. *Küberturvalisuse seaduse ja avaliku teabe seaduse muutmise seaduse eelnõu, Annex 2: eelnõu seletuskiri*. EIS document no. 21-0125/01 (01.02.2021). URL: https://eelnoud.valitsus.ee/main/mount/docList/3566abf6-2ad6-415d-9c0e-78d7fb7fb33f.

[42] Justiitsministeerium. *Küberturvalisuse seaduse ja avaliku teabe seaduse muutmise seaduse eelnõu*. EIS document no. 21-0125/04 (04.03.2021). URL: https://eelnoud.valitsus.ee/main/mount/docList/3566abf6-2ad6-415d-9c0e-78d7fb7fb33f.

[43] Majandus- ja Kommunikatsiooniministeerium. *Küberturvalisuse seaduse ja teiste seaduste muutmise seaduse eelnõu, Annex: seletuskiri*. EIS document no. 21-0125/05 (21.09.2021). URL: https://eelnoud.valitsus.ee/main/mount/docList/3566abf6-2ad6-415d-9c0e-78d7fb7fb33f.

[44] Justiitsministeerium. *Küberturvalisuse seaduse, avaliku teabe seaduse ja Eesti Rahvusringhäälingu seaduse muutmise seaduse eelnõu kooskõlastamine*. EIS document no. 21-0125/12 (04.01.2022). URL: https://eelnoud.valitsus.ee/main/mount/docList/3566abf6-2ad6-415d-9c0e-78d7fb7fb33f.

[45] Justiitsministeerium. *Eelnõu kooskõlastamine*. E-mail registered in Riigikantselei no 21-02006-2 (11.10.2021). URL: https://dhs.riigikantselei.ee/avalikteave.nsf/documents/NT0038A87A?open.

[46] Riigikogu riigikaitsekomisjon. *Riigikogu riigikaitsekomisjoni istungi protokoll nr 173 (14.03.2022)*. Registered in Riigikogu legislative file 531 SE. URL: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/cd3107f9-b19c-4ed4-b6a7-7379fa3bf6b9/.

[47] Riigikogu riigikaitsekomisjon. *Riigikogu riigikaitsekomisjoni istungi protokoll nr 193 (16.05.2022)*. Registered in Riigikogu legislative file 531 SE. URL: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/cd3107f9-b19c-4ed4-b6a7-7379fa3bf6b9/.

[48] Majandus- ja Kommunikatsiooniministeerium. *Küberturvalisuse seaduse ja teiste seaduste muutmise seadus (küberturvalisuse 2. direktiivi ülevõtmine), Annex 2: seletuskiri*. EIS document no. 24-1266/01 (09.12.2024). URL: https://eelnoud.valitsus.ee/main/mount/docList/c774c2e2-0c3e-4137-b24b-b49d1249f326.

[49] Eesti Linnade ja Valdade Liit. *Eelnõu kooskõlastamine*. EIS document no. 24-1266/03 (04.02.2025). URL: https://eelnoud.valitsus.ee/main/mount/docList/c774c2e2-0c3e-4137-b24b-b49d1249f326.

[50] Siseministeerium. *Vastuskiri*. EIS document no. 24-1266/06 (10.02.2025). URL: https://eelnoud.valitsus.ee/main/mount/docList/c774c2e2-0c3e-4137-b24b-b49d1249f326.

[51] Rahandusministeerium. *Küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõu kooskõlastamine*. EIS document no. 24-1266/08 (17.02.2025). URL: https://eelnoud.valitsus.ee/main/mount/docList/c774c2e2-0c3e-4137-b24b-b49d1249f326.

[52] Eesti Infotehnoloogia ja Telekommunikatsiooni Liit. *Arvamuse esitamine küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõu kohta*. E-mail registered in Justiits- ja Digiministeerium legistative file no 8-2/8641 (6.1-2/13 31.01.2025). URL: https://adr.rik.ee/jm/dokument/16587473.

[53] Riigikogu. *XV Riigikogu, VI istungjärk, täiskogu istung 23.10.2025*. Registered in Riigikogu legislative file 739 SE. URL: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/4429a2b9-e6e2-41cf-991d-f6955c6c4a69.

[54] Eesti Advokatuur. *Küberturvalisuse seaduse ja teiste seaduste muutmise seadus (küberturvalisuse 2. direktiivi ülevõtmine)*. E-mail registered in Justiits- ja Digiministeerium legistative file no 8-2/8641 (1-8/982-1 03.02.2025). URL: https://adr.rik.ee/jm/dokument/16587488.

[55] Riigi Teataja. *Küberturvalisuse seaduse ja teiste seaduste muutmise seadus (küberturvalisuse 2. direktiivi ülevõtmine)*. URL: https://www.riigiteataja.ee/akt/130122025004.

[56] Riigi Infosüsteemi Amet. *Eesti infoturbestandard (E-ITS)*. Accessed 31 March 2026. RIA. n.d. URL: https://www.ria.ee/kuberturvalisus/riigi-infoturbe-meetmete-haldus/eesti-infoturbestandard-e-its.

[57] John W. Meyer and Brian Rowan. „Institutionalized Organizations: Formal Structure as Myth and Ceremony“. In: *American Journal of Sociology* 83.2 (1977), pp. 340–363. DOI: 10.1086/226550. URL: http://www.iot.ntnu.no/innovation/norsi-pims-courses/harrison/Meyer%20&%20Rowan%20(1977).PDF.

[58] Michael Power. *The Audit Society: Rituals of Verification*. Oxford University Press, 1997. URL: https://vdoc.pub/download/the-audit-society-rituals-of-verification-57eue2suvt90.

[59] Patricia Bromley and Walter W. Powell. „From Smoke and Mirrors to Walking the Talk: Decoupling in the Contemporary World“. In: *The Academy of Management Annals* 6.1 (2012), pp. 483–530. DOI: 10.1080/19416520.2012.684462. URL: https://www.researchgate.net/publication/271936861_From_Smoke_and_Mirrors_to_Walking_the_Talk_Decoupling_in_the_Contemporary_World.

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis

I Anti Allikvee (09.03.1983)

1. grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Assessing the Administrative Implications of Estonian Regulatory Information Security Framework”, supervised by Kaido Kikkas , to be
    1.1. reproduced for the purposes of preservation and electronic publication, incl. to be entered in the digital collection of TalTech library until expiry of the term of copyright;
    1.2. published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of TalTech library until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1.
3. I confirm that granting the non-exclusive licence does not infringe third persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

14.05.2026

Appendix 2 – List of analysed acts and abbreviations

Short	Number	Link
E-ITS	16.12.2022 nr 101	Eesti infoturbestandard
E-ITS_1	E-ITS Lisa 1	Nõuded infoturbe halduse süsteemile
E-ITS_2	E-ITS Lisa 2	Etalonturbe kataloog
E-ITS_3	E-ITS Lisa 3	Auditeerimiseeskiri
KTN	09.12.2022 nr 121	Võrgu- ja infosüsteemide küberturvalisuse nõuded
KTN_1	KTN Lisa	Esmased turvameetmed
KüTS	09.05.2018	Küberturvalisuse seadus
PILV	03.01.2024 nr 1	Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel
RIHA	28.02.2008 nr 58	Riigi infosüsteemi haldussüsteem

Appendix 3 – Information Obligations

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
001	KüTS	§ 3^1(1)	A service provider and a domain name registration service provider **submit to the Estonian Information System Authority**, for the compilation of the list specified in subsection 2 of this section, at least the following information: 1. name and registry code; 2. the address of the place of business and up-to-date contact details, including e-mail addresses, Internet Protocol address ranges and telephone numbers; 3. where appropriate, the relevant sector and subsector 4. where appropriate, a list of the countries in which it provides services	Provide	one-off
002	KüTS	§ 3^1(4)	The service provider and the domain name registration service provider **notify the Estonian Information System Authority** of any changes to the information submitted pursuant to IO-ID 001 without delay, but no later than two weeks after the date on which the change was made.	Update	event-based
003	KüTS	§ 4(1)	A digital service provider **submits to the Estonian Information System Authority** at least the following information: 1. name and registry code; 2. where relevant, information on the relevant sector, subsector and type of entity 3. the address of its main place of business and the addresses of its other official places of business in the European Union or, if it has no place of business in the European Union or is not established there, the address of the place of business of its representative; 4. its up-to-date contact details and, where relevant, the up-to-date contact details of its representative, including the e-mail address and telephone number; 5. the Member State or Member States where the service is provided; 6. Internet Protocol address ranges.	Provide	event-based
004	KüTS	§ 4(6)	A digital service provider **notifies** of all changes to the information submitted pursuant to IO-ID 003 without delay, but no later than three months after the date on which the change was made.	Update	event-based
005	KüTS	§ 4(10)	A digital service provider providing services in Estonia but established outside the European Union must designate a representative in Estonia or in another Member State of the European Union where it provides the service or where it is established, and must **make the contact details** of the representative permanently publicly **available**.	Publish	one-off
006	KüTS	§ 6 p 3	the principle of minimising adverse effect – in the case of a cyber incident the service provider applies due care and measures to avoid the escalation of the effect of the cyber incident and its possible spread to another system and **notifies the supervisory authority** provided in this Act of the cyber incident;	Provide	event-based
007	KüTS	§ 6^1(1)	A service provider is to designate at least one member of the management board who approves the security measures, oversees their implementation and is responsible therefor. At the request of the Estonian Information System Authority, the service provider **submits the name and contact details** of the relevant member or members of the management board. The obligation to designate a responsible member of the management board does not apply to a service provider that has one member of the management board.	Provide	event-based
009	KüTS	7(1) 1	manage risks posed to the security of the system used in the activities of the service provider or in providing the service, including by **preparing a corresponding risk assessment**	Store	one-off
010	KüTS	§ 8(1)	A service provider, except for a security authority, **submits to the Estonian Information System Authority an initial notification** without delay, but no later than 24 hours after becoming aware of a cyber incident	Provide	event-based
011	KüTS	§ 8(1^1)	If a service provider authorises another person to manage the system or hosts the system with another person, the service provider is responsible for **ensuring that the other person notifies** the service provider no later than 24 hours after becoming aware of a cyber incident specified in subsection 1 of this section.	Provide	event-based
012	KüTS	§ 8(4^1)	A service provider, except for a security authority, **forwards to the Estonian Information System Authority** without delay, but no later than 72 hours after becoming aware of a cyber incident with a significant impact, an incident notification updating the information submitted in the initial notification in order to obtain a specified overview of the circumstances of the cyber incident with a significant impact.	Update	event-based
013	KüTS	§ 8(4^2)	A trust service provider **submits the incident notification** specified in IO-ID 012 of this section without delay, but no later than 24 hours after becoming aware of a cyber incident with a significant impact.	Provide	event-based
014	KüTS	§ 8(4^3)	At the request of the Estonian Information System Authority, a **service provider submits**, before submitting the final report specified in subsection 7 of this section, **an interim report** on the status of responding to the cyber incident with a significant impact. The interim report is to contain the data prescribed in the incident notification and, where relevant, additional information requested by the Estonian Information System Authority.	Provide	event-based
015	KüTS	§ 8(5)	Where relevant, a service provider is required to **inform**, within a reasonable time, a person who may be affected by a cyber incident with a significant impact or by a significant cyber threat, or the public if the affected persons cannot be informed individually. In the notification, the service provider, where possible, provides information about the significant cyber threat and the measures which the affected person may take in order to respond to the significant cyber threat.	Publish	event-based
016	KüTS	§ 8(6)	Where public awareness or the disclosure of a cyber incident is necessary to prevent or deal with a cyber incident with a significant impact or otherwise in the public interest, the Estonian Information System Authority may, after consulting the relevant service provider, **inform the public** of the cyber incident with a significant impact or **require the relevant service provider** to do so.	Publish	event-based
017	KüTS	§ 8(7)	A service provider **submits a final report** to the Estonian Information System Authority within one month as of the submission of the incident notification specified in subsection 41 of this section. If the cyber incident with a significant impact has not yet been resolved by the time the final report is submitted, the submitted final report is treated as an interim report and the service provider submits a new final report within one month after the cyber incident with a significant impact has been resolved.	Provide	event-based
018	PILV	§ 2(7)	(1) Teabepidaja, kes soovib avaliku teabe töötlemiseks kasutusele võtta avaliku sektori osutatava pilvteenuse või pilvandmetöötlusteenuse (edaspidi koos pilvteenus), peab hindama muu hulgas: (7) Teabepidaja **dokumenteerib** lõikes 1 ette nähtud hindamise enne, kui hakkab pilvteenust kasutama. Teabepidaja võib dokumenteerimise teha muu õigusakti alusel koostatava dokumentatsiooni osana.	Store	one-off
019	PILV	§ 3(2)	(1) Enne, kui avaliku teabe töötlemiseks võetakse kasutusele pilvteenus, määratakse kindlaks järgmine: (2) Lõikes 1 sätestatu, sealhulgas mõlema poole õigused ja kohustused, **fikseerivad** teabepidaja ja avaliku sektori pilvteenuse pakkuja või pilvandmetöötlusteenuse pakkuja või tema volitatud esindaja, importija või levitaja **kirjalikult taasesitatavas vormis**.	Store	one-off
020	PILV	§ 3(4)	Pilvteenuse kasutamise alustamisest **teavitab** teabepidaja, välja arvatud julgeolekuasutus, viivitamata Riigi Infosüsteemi Ametit. Julgeolekuasutusest teabepidaja teavitab viivitamata küberturvalisuse seaduse § 14 lõikes 5 nimetatud haldusjärelevalve tegijat.	Provide	event-based
021	PILV	§ 4(2)	Kui § 2 lõigetes 1 **[IO-ID 018]**, 3 ja 5 sätestatud asjaolud muutuvad, **hinnatakse** muutust ja selle mõju pilvteenuse kasutamisele. Muutust hinnatakse enne muutuse toimumist või 30 päeva jooksul muutusest teada saamisest arvates.	Update	event-based

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
022	PILV	§ 4(3)	Paragrahvi 3 lõikes 5 **[IO-ID 020]** sätestatud asjaolude muutumise korral **teavitab** teabepidaja, välja arvatud julgeolekuasutus, viivitamata Riigi Infosüsteemi Ametit. Julgeolekuasutusest teabepidaja teavitab küberturvalisuse seaduse § 14 lõikes 5 nimetatud haldusjärelevalve tegijat.	Provide	event-based
023	PILV	§ 5(4)	Pilvteenuse kasutamise lõppemisest **teavitab** teabepidaja, välja arvatud julgeolekuasutus, viivitamata Riigi Infosüsteemi Ametit. Julgeolekuasutusest teabepidaja teavitab küberturvalisuse seaduse § 14 lõikes 5 nimetatud haldusjärelevalve tegijat.	Provide	event-based
024	KTN	§ 4(2)	Teenuse osutaja **edastab** lõike 1 või 1^1 alusel läbi viidud **[Eesti infoturbestandardi tingimuste täitmise] auditi** järeldusotsuse Riigi Infosüsteemi Ametile 30 päeva jooksul selle kättesaamisest.	Provide	event-based
025	KTN	§ 5(1)	Teenuse osutaja kaardistab süsteemid ja nendega seotud teenused või protsessid ning **dokumenteerib** süsteemile rakendatavad turvameetmed ja riskianalüüsi.	Store	one-off
027	KTN	§ 5(2)	Teenuse osutaja säilitab lõikes 1 nimetatud dokumentatsiooni vähemalt seitse aastat alates selle koostamisest ning **teeb** selle Riigi Infosüsteemi Ametile taotluse korral **kättesaadavaks.**	Make available	event-based
028	KTN	§ 6	Teenuse osutaja ajakohastab riskianalüüsi: 1. viivitamata pärast olulise mõjuga küberintsidendi toimumist; 2. viivitamata pärast teenuse osutamiseks kasutatava süsteemi sellist muutust, mis mõjutab süsteemi turvalisust, või 3. hiljemalt kolme aasta möödumisel viimasest ajakohastamisest.	Update	event-based; periodic
031	RIHA	§ 6(2)	Kui kontrolli tulemusel selgub, et vajalike andmete kogumiseks või töötlemiseks on otstarbekas asutada uus andmekogu või muuta olemasolevas andmekogus kogutavate andmete koosseisu, **koostab** andmekogu asutaja või vastutav töötleja andmekogu **dokumentatsiooni**.	Store	event-based
032	RIHA	§ 6(4)	Kui kontrolli tulemusel selgub, et vajalikke andmeid kogutakse juba mõne asutatud andmekogu koosseisus, **esitab** uue andmekogu asutaja RIHA kaudu selle andmekogu vastutavale töötlejale **taotluse** andmete kättesaadavaks tegemiseks riigi infosüsteemis.	Provide	event-based
033	RIHA	§ 7(1)	Andmekogu asutamisel või andmekogus kogutavate andmete koosseisu muutmisel **esitab** andmekogu vastutav või volitatud töötleja andmekogu **dokumentatsiooni** RIHA kaudu ühel ajal kooskõlastamiseks Riigi Infosüsteemi Ametile, Andmekaitse Inspektsioonile, Statistikaametile, Maa- ja Ruumiametile ning Rahvusarhiivile, arvestades lõikes 2 toodud erisusi.	Provide	event-based
034	RIHA	§ 7(9)	Kui pärast andmekogu dokumentatsiooni kooskõlastamist ning enne andmekogu või andmekogus kogutavate andmete koosseisu muutmise registreerimist tehakse andmekogu dokumentatsioonis **muudatusi**, tuleb see **esitada** käesolevas paragrahvis sätestatud korras uuesti **kooskõlastamiseks** lõikes 1 nimetatud asutustele.	Provide	event-based
035	RIHA	§ 10(2)	Andmekogu vastutav või volitatud töötleja **esitab** andmekogu ja andmekogus kogutavate andmete koosseisu **muutmise** registreerimiseks RIHA-s pärast andmekogu asutamise või andmekogus kogutavate andmete koosseisu muutmise aluseks oleva õigusakti vastuvõtmist, kuid mitte hiljem kui 10 tööpäeva jooksul pärast vastava õigusakti jõustumist.	Provide	event-based
036	RIHA	§ 10(3)	Andmekogu registreerimisel ja andmekogus kogutavate andmete koosseisu muutmise registreerimisel tuleb andmekogu vastutaval või volitatud töötlejal **aktualiseerida** kõik ... andmete koosseisule vastavad **andmed**.	Update	event-based
037	RIHA	§ 11	Kui andmekogu muudatused ei ole seotud andmekogusse kogutavate andmete koosseisuga, ei ole vaja neid muudatusi §-s 7 sätestatud korras kooskõlastada. Sellised muudatused **registreerib** andmekogu vastutav või **volitatud töötleja** RIHA-s.	Update	event-based
038	RIHA	§ 12(1)	Andmekogu tegevuse lõpetamisel otsustatakse andmete üleandmine teise andmekogusse, arhiivi või nende kuulumine hävitamisele ning üleandmise või hävitamise tähtaeg. Andmete üleandmisel või hävitamisel **koostatakse vastav akt**, mis kantakse andmekogu tegevuse lõpetamise registreerimisel **RIHA**-sse.	Store	event-based
039	RIHA	§ 12(2)	Andmekogu tegevuse lõpetamisest **teavitab** andmekogu **vastutav töötleja** RIHA kaudu Riigi Infosüsteemi Ametit, Andmekaitse Inspektsiooni, Statistikaametit, Maa- ja Ruumiametit ja Rahvusarhiivi. Riigi Infosüsteemi Ametil ja Andmekaitse Inspektsioonil on õigus nõuda andmete üleandmist või hävitamist nende volitatud ametiisikute juuresolekul.	Provide	event-based
040	RIHA	§ 13(2)	Andmekogu asutaja või vastutav või volitatud töötleja kõrvaldab keeldumise aluseks olnud asjaolud ning **esitab** andmekogu **uueks registreerimiseks** RIHA-s.	Update	event-based
041	E-ITS_1	6.1	Infoturvapoliitika [**koostamine**]	Store	one-off
042	E-ITS_1	6.1.6	Infoturvapoliitika kinnitab juhtkond. Infoturvapoliitika **tehakse teatavaks** töötajatele ning vajadusel teistele huvipooltele.	Make available	event-based
043	E-ITS_1	6.1.7	Organisatsioon **vaatab** infoturvapoliitika perioodiliselt või oluliste muutuste korral **üle** ja ajakohastab vajadusel.	Update	periodic; event-based
044	E-ITS_1	6.2.3(a)	**kirjeldab äriprotsessid** ja võtab arvele varad	Store	one-off
045	E-ITS_1	6.2.3(a)	kirjeldab äriprotsessid ja **võtab arvele varad**	Store	one-off
045-1	E-ITS_1	6.2.3(b)	**määrab** organisatsiooni infoturbe **kaitseala** ja sihtobjektid	Store	one-off
045-2	E-ITS_1	6.2.3(d)	**määrab** sihtobjektide **kaitsetarbe** skaalal „normaalne", „suur", „väga suur";	Store	one-off
046	E-ITS_1	6.2.3(e)	**dokumenteerib** infoturvaeesmärgid ja määrab eesmärkide saavutamise ajaraamid	Store	one-off
047	E-ITS_1	6.2.4	Organisatsioon sõnastab infoturvaeesmärgid, **vaatab neid regulaarselt läbi ja vajadusel ajakohastab**	Update	periodic
048	E-ITS_1	6.3.5	Turbekorraldus tehakse töötajatele **teatavaks**.	Make available	event-based
049	E-ITS_1	6.7.2	Organisatsioon **kehtestab** dokumentide koostamise, vormistamise ja hoidmise reeglid.	Store	one-off
050	E-ITS_1	6.7.3	Poliitikad ja eeskirjad **vaadatakse üle** vähemalt üks kord aastas ning muudatused kinnitab juhtkond. Korrad ja protseduurijuhendid hoitakse tegelike protsessidega kooskõlas.	Update	periodic
051	E-ITS_1	6.7.4	Organisatsioon **loob ja säilitab** tegevusdokumentatsiooni, mis tekib või luuakse infoturbeprotsessi käigus.	Store	event-based
052	E-ITS_1	6.7.5(a)	**Dokumenteeritakse**: a) infoturbeprotsessi alusdokumendid ja nende väljatöötamise kulg konteksti jäädvustamiseks	Store	event-based
053	E-ITS_1	6.7.5(b)	**Dokumenteeritakse**: b) otsused, sh infoturbe meetmete rakendusplaan, et tagada otsuste ja meetmete rakendamise käigu jälitatavus (ingl traceability)	Store; Update	event-based
054	E-ITS_1	6.7.5(c)	**Dokumenteeritakse**: c) infoturbesündmused sisendiks riskihaldusse infoturbe täiustamiseks	Store	event-based
055	E-ITS_1	6.7.5(d)	**Dokumenteeritakse**: d) organisatsiooni reaktsioon sündmustele ja otsustele, et näidata parandusmeetmete toimivust	Store	event-based
056	E-ITS_1	6.7.6	Infoturbeprotsessi dokumentatsioon on volitatuile **kättesaadav** ja kaitstud kõrvalise juurdepääsu eest.	Make available	event-based

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
057	E-ITS_1	7.1.3	Kaitsealasse kuuluvate sihtobjektide kaitsetarve tuvastatakse ja **dokumenteeritakse**, sh määratakse kaitsetarve väljast tellitavatele teenustele (tarneahel).	Store	event-based
058	E-ITS_1	7.1.4	Riskihalduse käik ja tuvastatud või määratud meetmete rakendamise otsused **dokumenteeritakse** korratavuse ja võrreldavuse eesmärgil.	Store	event-based
059	E-ITS_1	7.3.2	Organisatsioon määrab etalonturbe välise riskihalduse protsessi. Riskihalduse asjaolud, kulg ja tulemused **dokumenteeritakse**.	Store	event-based
060	E-ITS_1	8.6	Organisatsiooni juhtkond teadvustab ja **aktsepteerib regulaarselt** jääkriskid ning nende alusel **kinnitab** rakendusplaani.	Update	periodic
061	E-ITS_1	8.8	Organisatsioon **tagab** meetmetes kirjeldatud korduvate ja regulaarsete tegevuste tõendatavuse, võrreldavuse, järjepidevuse ja õigeaegsuse.	Store	periodic
062	E-ITS_1	9.3	Seiratakse protsesside ja süsteemide töö käigus tekkinud teavet. Olulistele infoturbe sündmustele reageeritakse ja need **registreeritakse**.	Store	event-based
063	E-ITS_1	9.4	Seire, ülevaatuste ja kontrollide **dokumenteeritud** tulemusi ja järeldusi kasutab organisatsioon riskihalduses ettepanekute koostamiseks infoturbeprotsessi ja -meetmete täiustamiseks ning muutmiseks.	Store	periodic
064	E-ITS_1	10.2.5	Läbivaatuste tulemused ja ettepanekud **dokumenteeritakse** täiustamise ja jälitatavuse eesmärgil. Tulemusi arvestatakse organisatsiooni protsesside täiustamisel.	Store	periodic
065	E-ITS_1	11.4	E-ITS auditi järeldusotsus on **tõend** organisatsiooni infoturbe toimivuse kohta.	Store	one-off
066	E-ITS_3	5.2	E-ITS auditi käsitlusala on üheselt arusaadavalt piiritletud ja **dokumenteeritud**.	Store	one-off
067	E-ITS_3	5.4.7	riskihalduse metoodika **koostamine** ja kehtestamine	Store	one-off
068	E-ITS_3	5.4.8	äriprotsessidega seotud infotehnoloogia (edaspidi IT) riskide kaalutlemine (IT riskianalüüsi **koostamine**)	Store	one-off
069	E-ITS_3	5.4.9	infoturbe meetmete rakendusplaani (IMR) **koostamine**	Store	one-off
071	E-ITS_3	6.2	E-ITS auditi läbiviimiseks **sõlmitakse** audiitorettevõttega auditeerimisleping	Store	one-off
072	E-ITS_3	6.4	Enne auditiprotseduuridega alustamist **sõlmitakse** audiitorettevõtte ja auditeeritava organisatsiooni vahel konfidentsiaalsusleping.	Store	one-off
073	E-ITS_3	7.4	Kui käsitlusalasse kuuluvaid andmeid töödeldakse mitmes erinevas asukohas, esitab E-ITS auditi tellija **hankekutses** ...	Publish	event-based
074	E-ITS_3	7.7	Kui organisatsioon vahetab audiitorettevõtet, lisab ta **hankedokumentatsiooni** E-ITS auditi kehtiva järeldusotsuse.	Store	event-based
075	E-ITS_3	8.8	Auditirühma liikmete sõltumatus peab olema **kinnitatud** allkirjastatud deklaratsiooniga.	Store	one-off
076	E-ITS_3	9.3	Audiitor **toob** E-ITS **eelauditi aruandes välja** puudused ning esitab soovitused E-ITS auditi eeldustena käsitletavate toimingute sooritamiseks.	Store	one-off
077	E-ITS_3	10.2	Enne E-ITS põhiauditi läbiviimist **koostatakse** ja kooskõlastatakse auditeeritava organisatsiooniga E-ITS auditi plaan. Auditi plaan aitab tagada, et kriitilistele kontrollivaldkondadele pööratakse auditi käigus piisavalt tähelepanu ja auditiprotseduurid tehakse õiges järjekorras. Olude muutudes või ootamatute asjaolude ilmnedes muudetakse vastavalt ka auditi plaani.	Store; Update	event-based
078	E-ITS_3	10.11	E-ITS põhiaudit lõpeb auditi lõpparuande ja järeldusotsuse **esitamisega**	Provide	event-based
079	E-ITS_3	11.4	E-ITS vaheauditite kavandamise etapis **teavitab** auditeeritav organisatsioon E-ITS audiitorit muudatustest organisatsiooni äriprotsessides, IT-süsteemides tehtud muudatustest ja toimunud infoturbe intsidentidest, mis võivad mõjutada vaheauditi käsitlusala.	Provide	event-based
080	E-ITS_3	11.5	E-ITS vaheauditi käigus tehtud tähelepanekud **vormistab** audiitor E-ITS vaheauditi aruandena lähtudes lõpparuande ja järeldusotsuse nõuetest	Store	event-based
081	E-ITS_3	12.11	E-ITS auditi käigus tehtud leidude kohta on audiitoril olemas **tõendusmaterjal**, auditi testid on korratavad.	Store	event-based
082	E-ITS_3	12.13	Enne E-ITS auditi lõpparuande kinnitamist **esitatakse** auditeeritava organisatsiooni esindajale E-ITS auditi aruande kavand.	Provide	event-based
083	E-ITS_3	12.14	E-ITS põhiauditi lõpparuanne esitatakse hiljemalt üks kuu pärast audititoimingute lõpetamist. Auditeeritav organisatsioon **kinnitab** E-ITS auditi aruande vastuvõtmise kirjalikult taasesitatavas vormis.	Provide	event-based
084	E-ITS_3	12.17	Järelevalveasutusele **esitab** E-ITS auditi aruande ja E-ITS auditi järeldusotsuse E-ITS auditi tellija.	Provide	event-based
085	E-ITS_3	13.4	Kõrge riskiastmega lahknevuste kohta tellib auditeeritav organisatsioon E-ITS **järelauditi [koostab aruande]**.	Store	event-based
087	E-ITS_3	13.6	Audiitor **säilitab** E-ITS auditi aruandeid ja seonduvaid tööpabereid turvaliselt, vastavalt poolte vahelisele kokkuleppele. Juurdepääs dokumentidele on lubatud üksnes vastava pääsuõigusega isikul.	Store	event-based
088	KTN_1	1.2	**välja töötama** võrgu- ja infosüsteemide turvareeglid, sealhulgas infoturbepõhimõtted, ning tutvustama neid personalile	Store; Make available	one-off
090	KTN_1	1.4	**pidama** infotehnoloogiavarade arvestust ning uuendama seda regulaarselt	Store; Update	periodic
091	KTN_1	2.1	**tutvustama** personalile küberhügieeni- ja infoturbereegleid, hindama teadmisi ja tagama talle vastava koolituse, vajaduse korral perioodiliselt	Make available	periodic
092	KTN_1	3.2	**välja töötama** tööks vajalike andmete kasutamise reeglid, sealhulgas teiste isikutega andmete jagamise kohta	Store	one-off
093	KTN_1	4.2	**kokku leppima** tarnijatega, väliste teenuste osutajatega ja partneritega kirjalikult taasesitatavas vormis andmete vahetamiseks vajalikud turvanõuded ning kasutatava teenuse tingimused	Store	event-based
094	KTN_1	6.6	**pidama nimekirja** kõigist kasutuses olevatest pilvteenustest koos teenuse pakkuja, kasutusotstarbe ja riskihinnangu kokkuvõttega	Store	event-based
095	KTN_1	7.3	**pidama arvestust** kasutatava tarkvara, tarkvara nõrkuste ja litsentside üle ning uuendama litsentse õigel ajal	Store; Update	event-based
096	KTN_1	8.1	**koostama** arvutivõrgu skeemi, sealhulgas pidama võrguseadmete ning võrgule tuge pakkuvate isikute ja nende kontaktandmete arvestust	Store	one-off
097	KTN_1	8.1	koostama arvutivõrgu skeemi, sealhulgas **pidama** võrguseadmete ning võrgule tuge pakkuvate isikute ja nende kontaktandmete **arvestust**	Store; Update	event-based
098	KTN_1	9.4	**pidama arvestust** ruumidele, sõidukitele, hoonetele ja muule varale juurdepääsu võimaldavate vahendite üle, sealhulgas kaardid, koodid ja võtmed	Store; Update	event-based
099	E-ITS_2	ISMS.1.M2(b)	Infoturbe eesmärgid on **dokumenteeritud**. Eesmärgid on realistlikud, praktilised, põhjendatud ja arusaadavad.	Store	one-off
100	E-ITS_2	ISMS.1.M3(b)	Organisatsiooni juhtkond kinnitab ja **kehtestab** infoturvapoliitika	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
101	E-ITS_2	ISMS.1.M3(e)	Infoturvapoliitika **tehakse teatavaks** kõigile töötajatele ja organisatsiooni partneritele, vajadusel ka avalikkusele. Juurdepääs olulisele teabele võimaldatakse töötajatele ja partneritele üksnes pärast poliitika aktsepteerimist.	Make available	event-based
102	E-ITS_2	ISMS.1.M3(f)	Infoturvapoliitikat **ajakohastatakse** regulaarselt või oluliste muudatuste puhul infotehnoloogia (edaspidi IT) süsteemides, organisatsiooni eesmärkides või turbe strateegias	Update	event-based; periodic
103	E-ITS_2	ISMS.1.M5(d)	Välise infoturbejuhiga on **sõlmitud** konfidentsiaalsusleping	Store	one-off
104	E-ITS_2	ISMS.1.M6(a)	Organisatsiooni juhtkond **kehtestab** infoturbe korralduse organisatsioonis ja tagab selleks vajalikud ressursid (raha, tööjõud, vahendid)	Store	one-off
105	E-ITS_2	ISMS.1.M7(b)	Rakendatavad turvameetmed on süsteemselt **dokumenteeritud**, vajadusel meetme rakenduse kirjeldust ajakohastatakse	Store	event-based
106	E-ITS_2	ISMS.1.M7(c)	Määratud, kuid rakendamata jäetud meetme puhul: • on **tehtud täiendav riskianalüüs**, mis on aluseks juhtkonnale riski aktsepteerimise või mitteaktsepteerimise osas; • on dokumenteeritud mitterakendamise põhjus ja asjaolud.	Store	event-based
107	E-ITS_2	ISMS.1.M7(c)	Määratud, kuid rakendamata jäetud meetme puhul: • on tehtud täiendav riskianalüüs, mis on aluseks juhtkonnale riski aktsepteerimise või mitteaktsepteerimise osas; • on **dokumenteeritud** mitterakendamise põhjus ja asjaolud.	Store	event-based
109	E-ITS_2	ISMS.1.M10(a)	Infoturbe strateegia elluviimiseks ja infoturbe eesmärkide täitmiseks on **välja töötatud** turbekontseptsioon (ingl security concept). Turbekontseptsioon on turbeprotsessi alusdokument. Organisatsioonis võib olla samaaegselt mitu erinevat turbekontseptsiooni, mis rakenduvad organisatsiooni eri osadele.	Store	one-off
110	E-ITS_2	ISMS.1.M11(d)	Turvaläbivaatuse tulemused **dokumenteeritakse** ning lahknevuste põhjused selgitatakse. Läbivaatuse käigus ilmnenud puuduste parandusmeetmed **dokumenteeritakse**.	Store	event-based
111	E-ITS_2	ISMS.1.M11(e)	Väliste kontrollijate puhul lepitakse kokku kohustused ja aruandlus ning **sõlmitakse** konfidentsiaalsuslepe.	Store	one-off
112	E-ITS_2	ISMS.1.M12(a)	Juhtkonnale **esitatakse** regulaarselt aruandeid infoturbe olukorrast, eelkõige riskiseisu ning turbeprotsessi toimivuse ja tõhususe kohta.	Store	periodic
113	E-ITS_2	ISMS.1.M12(b)	Infoturbearuanne **esitatakse** lisaks sündmusepõhiselt, nt pärast turvaintsidenti või turbeprotsessi olulises punktis	Provide	event-based
114	E-ITS_2	ISMS.1.M12(d)	Juhtkonna otsused turvameetmete, jääkriskide ja turbeprotsesside muutmise kohta on jälitatavalt **dokumenteeritud**.	Store	event-based
115	E-ITS_2	ISMS.1.M13(a)	Turbeprotsessi protseduurid, olulised otsused ja tegevuste tulemused on **dokumenteeritud**. Kindlasti dokumenteeritakse järgmine: • aruanded juhtkonnale (vt ISMS.1.M12 Infoturbearuanded juhtkonnale); • turbeprotsessi korralduse dokumentatsioon; • turbetegevuste dokumentatsioon; • turvaintsidentide dokumentatsioon; • tehniline dokumentatsioon (nt tehnilised juhendid, testimistulemid, rakenduste kasutusload); • protsessijuhendid töötajatele.	Store; Update	event-based
116	E-ITS_2	ISMS.1.M13(b)	**On olemas** reeglistik dokumentatsiooni koostamiseks, hoidmiseks ning dokumentatsiooni ajakohasuse ja konfidentsiaalsuse tagamiseks.	Store	one-off
117	E-ITS_2	ISMS.1.M16(a)	Kitsama käsitlusalaga turvapoliitika **koostatakse** vähemalt järgmistes valdkondades: • võrguhaldus; • tulemüüri haldus; • kahjurvaratõrje; • andmevarundus ja arhiveerimine; • e-post ja rühmatarkvara; • mobiilseadmete kasutamine; • teenuste väljasttellimine.	Store	event-based
118	E-ITS_2	ORP.1.M1(b)	Eeskirjadega **kehtestatakse** turbe korraldus vähemalt järgmistes valdkondades: • varundus ja arhiveerimine; • andmekandjate käitus; • hoolde- ja remonditööd; • andmekaitse; • avariivalmendus.	Store	one-off
119	E-ITS_2	ORP.1.M1(c)	Eeskirjad **tehakse teatavaks** kõigile töötajaile ning neid vaadatakse regulaarselt üle.	Make available	periodic
120	E-ITS_2	ORP.1.M8(d)	Töövahendite ja seadmete turvaliseks kasutuselt kõrvaldamiseks on **koostatud** juhendid ja soetatud vajalikud vahendid (nt dokumendipurusti). Andmekandjad kõrvaldatakse vastavalt moodulile CON.6. Andmete kustutus ja hävitamine.	Store	one-off
121	E-ITS_2	ORP.1.M16(a)	Organisatsioonis on **kehtestatud** IT-vahendite turvalise kasutamise eeskiri.	Store	one-off
122	E-ITS_2	ORP.1.M16(d)	Uus töötaja **kinnitab** enne IT-vahendite kasutuselevõttu **kirjalikult**, et on eeskirjaga tutvunud.	Store	event-based
123	E-ITS_2	ORP.1.M16(e)	IT- vahendite turvalise kasutamise eeskirja **vaadatakse üle** perioodiliselt ning pärast oluliste muudatuste tegemist IT-süsteemides	Update	periodic; event-based
124	E-ITS_2	ORP.2.M1(b)	On **koostatud** kontroll-loend, mis sisaldab kõiki uue töötaja töö alustamiseks vajalikke tegevusi.	Store	one-off
125	E-ITS_2	ORP.2.M2(h)	Tegevuste koordineerimiseks töötaja lahkumise korral kasutatakse sarnaselt töölevõtmisele asjakohast kontroll-loendit.	Store	event-based
126	E-ITS_2	ORP.2.M3(a)	Juhtkond on **koostanud** töötaja asendamise korra ja loonud eeldused selle järgimiseks. Asendamise kord eksisteerib tööülesannetele kõigis olulistes äriprotsessides.	Store	one-off
127	E-ITS_2	ORP.2.M5(a)	Organisatsioonivälise isikuga **sõlmitakse** kirjalik konfidentsiaalsusleping enne, kui talle antakse juurdepääs konfidentsiaalsele teabele	Store	one-off
128	E-ITS_2	ORP.2.M14(b)	Töötaja tööülesanded ja kohustused on **dokumenteeritud** ja neid on töötajale tutvustatud. Töötajad kinnitavad nõuete järgimist, allkirjastades vastava kontroll-loetelu.	Store	one-off
129	E-ITS_2	ORP.3.M3(c)	Organisatsioon on **koostanud** eeskirjad IT-, tööstusautomaatika ja esemevõrgu komponentide turvaliseks kasutamiseks. Eeskirjad on arusaadavad ja ajakohased, kohustuste selgeks määratlemiseks on need kinnitatud juhtkonnas.	Store	one-off
130	E-ITS_2	ORP.3.M4(a)	Töötajate teadlikkuse suurendamiseks on **välja töötatud** ja juhtkonna poolt kinnitatud infoturbe teadvustus- ja koolitusplaan.	Store	one-off
131	E-ITS_2	ORP.4.M1(a)	Organisatsioon on **koostanud** ja kinnitanud kasutajakontode halduse eeskirja.	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
132	E-ITS_2	ORP.4.M3(a)	Kasutajakontod, moodustatud kasutajarühmad ja õiguste profiilid **dokumenteeritakse**.	Store	event-based
133	E-ITS_2	ORP.4.M5(b)	Sissepääsuvahendina kasutatavate pääsmike (ingl security token) väljaandmine või kehtetuks muutmine **dokumenteeritakse**.	Store	event-based
134	E-ITS_2	ORP.4.M6(b)	Juurdepääsuvahendina kasutatavate kiipkaartide vm pääsmike väljaandmine või kehtetuks muutmine **dokumenteeritakse**.	Store	event-based
135	E-ITS_2	ORP.4.M7(b)	Kui andmetele juurdepääsuks kasutatakse pääsmikku, siis selle väljaandmine või kehtetuks muutmine **dokumenteeritakse**	Store	event-based
136	E-ITS_2	ORP.4.M8(a)	Organisatsioonis on **kehtestatud** paroolide kasutamise kord (vt ka ORP.4.M22 Parooli kvaliteedinõuete kehtestamine).	Store	one-off
136-1	E-ITS_2	ORP.4.M12(a)	Organisatsioonis on iga IT-süsteemi ja rakenduse jaoks määratud autentimisnõuded ja **kehtestatud** autentimiskord.	Store	one-off
137	E-ITS_2	ORP.4.M15(a)	Organisatsioonis on **koostatud** ja rakendatud protseduurid: • pääsupoliitikate haldamiseks; • kasutajakontode ja kasutajarühmade haldamiseks; • õiguste profiilide ja kasutajarollide haldamiseks.	Store	one-off
138	E-ITS_2	ORP.4.M16(c)	Iga IT-süsteemi juurdepääsude haldamiseks on **kehtestatud** protseduurid.	Store	one-off
139	E-ITS_2	ORP.4.M18(c)	Enne teenuse kasutuselevõttu on kavandatud ja **dokumenteeritud** keskse autentimisteenuse turvanõuded.	Store	event-based
140	E-ITS_2	ORP.5.M1(a)	Organisatsioonis on välja töötatud protsess kõigi turbehaldusele mõju avaldavate õigusaktide, lepingute ja muude nõuete väljaselgitamiseks. Asjakohased nõuded **dokumenteeritakse**.	Store	one-off; event-based
141	E-ITS_2	CON.1.M4(a)	Krüptograafiliste vahendite krüptovõtmete halduseks on **kehtestatud** sobiv võtmehaldussüsteem ja loodud turvaline keskkond.	Store	one-off
142	E-ITS_2	CON.1.M10(a)	Organisatsiooni krüptokontseptsiooni **loomisel** on lähtutud organisatsiooni üldisest turvapoliitikast. Krüptokontseptsioon esitab kasutatavate krüptomehhanismide ja krüptograafiliste vahendite tehnilised ja korralduslikud nõuded.	Store	one-off
143	E-ITS_2	CON.1.M19(a)	Organisatsioon on **loonud** kasutatavate krüptograafiliste vahendite (s krüptograafiliste funktsioonidega riist- ja tarkvara) loendi. Loend sisaldab vähemalt järgmist: • IT-süsteemid, mis antud krüptograafilist vahendit kasutavad; • krüptograafilise vahendi kasutamise eesmärk (n arvuti kõvaketta krüpteerimine); • krüptograafilised meetodid ja krüptomehhanismid; • krüptograafilise vahendi turvaparameetrid (n võtme pikkus).	Store	event-based
144	E-ITS_2	CON.1.M18(b)	**On olemas** krüptograafiliste funktsioonidega riistvara asendamist kirjeldavad juhendid.	Store	one-off
145	E-ITS_2	CON.2.M1(b)	Organisatsioon on kaardistanud ning **dokumenteerinud** õigusaktidest ning kolmandate pooltega sõlmitud lepingutest tulenevad andmekaitsenõuded.	Store	event-based
146	E-ITS_2	CON.2.M3(b)	Kaardistamise tulemused on **dokumenteeritud** isikuandmete töötlemise ülevaates.	Store	one-off
147	E-ITS_2	CON.2.M4(a)	Organisatsioon on **välja töötanud** ja kehtestanud andmekaitsepoliitika ja andmekaitsejuhised.	Store	one-off
148	E-ITS_2	CON.2.M7(a)	Organisatsioon on **koostanud** andmekaitsetingimused vastavalt IKÜM artikli 5 lõike 1 punktile a ja lõigetele 2, 12-22 ning arvestades põhjenduspunkte 39, 58-72 või vastavalt isikuandmete kaitse seaduse §-le 23 või vastavalt muule asjaomasele seadusele.	Store	one-off
149	E-ITS_2	CON.2.M8(b)	Andmesubjektidele **antakse** selget ja arusaadavat teavet nende õiguste kohta.	Provide	event-based
150	E-ITS_2	CON.2.M13(a)	Organisatsioon on **koostanud** andmekaitsealase mõjuhinnangu, kui see on IKÜM artiklist 35 või isikuandmete kaitse seaduse §-st 38 või muus asjaomasest seadusest tulenevalt nõutav. Andmekaitsespetsialist on mõjuhinnangu koostamisel nõustavas rollis.	Store	event-based
151	E-ITS_2	CON.2.M13(b)	Andmekaitsespetsialist või organisatsiooni juhtkond on **kehtestanud** mõjuhinnangu koostamise juhendi, mille alusel oskavad mõjuhinnangut teha ka ilma eelneva põhjaliku ettevalmistuseta töötajad.	Store	one-off
152	E-ITS_2	CON.2.M14(a)	Organisatsioon on volitatud töötlejaga **sõlminud** IKÜMist või seadusest või muust õigusaktist tuleneva andmetöötluslepingu. Andmetöötluslepingut ei sõlmita, kui andmeid töödeldakse Euroopa Liidu või selle liikmesriigi õiguse kohase siduva õigusakti alusel.	Store	event-based
153	E-ITS_2	CON.2.M16(a)	Organisatsioon on **koostanud** eeskirja, mis kirjeldab, kuidas ja kui kaua erinevaid isikuandmeid säilitatakse ning kuidas toimub isikuandmete kustutamine või andmekandjate hävitamine.	Store	one-off
154	E-ITS_2	CON.2.M19(a)	Kõik isikuandmete töötlemise toimingud **logitakse**	Store	event-based
155	E-ITS_2	CON.2.M20(d)	Organisatsioon on **koostanud** protseduurid külaliste haldamiseks, kes sisenevad organisatsiooni aladele, kus töödeldakse isikuandmeid. See hõlmab nii külaliste registreerimist, külastuste eelnevat kooskõlastamist, külaliste juhendamist organisatsiooni reeglite osas ning külastaja saatmist (st. külastaja liigub organisatsioonis ainult koos organisatsiooni töötajast saatjaga).	Store	one-off
156	E-ITS_2	CON.2.M23(a)	Organisatsioon on **koostanud** põhimõtted rakenduste testimise läbiviimiseks, milles keelatakse isikuandmete avaldamine, volitamata juurdepääs isikuandmetele ning piiratakse testijate tegevust isikuandmetega seotud süsteemides. Testimise all peetakse silmas nii rakenduste kasutuselevõtueelset testimist kui rakenduse läbistustestimisi turvanõrkuste avastamiseks.	Store	one-off
157	E-ITS_2	CON.2.M24(b)	Veebilehe külastajatele on kasutavate küpsiste ja jälgimisvahendite kohta **antud** selge ja üheselt mõistetav teave. Kui on nõutud, küsitakse küpsiste kasutamiseks veebilehe külastajalt nõusolekut	Provide	event-based
158	E-ITS_2	CON.2.M24(d)	Organisatsioon on veebilehel **avalikustanud** andmekaitsetingimused, mis kirjeldavad, milliseid isikuandmeid kogutakse (sh. küpsised), kuidas neid töödeldakse, millistel eesmärkidel, kaua säilitatakse ja kuidas privaatsust kaitstakse. Täiendavate andmekaitsetingimuste elementide koostamisel tuleb lähtuda IKÜM artiklitest 12-22 või asjaomasest seadusest.	Make available	one-off
159	E-ITS_2	CON.2.M25(a)	Organisatsioon on **kehtestanud** eeskirjad isikuandmete käitlemiseks ja kustutamiseks arvutitöökohtadel.	Store	one-off
160	E-ITS_2	CON.3.M1(g)	Andmevarunduse mõjurid on **dokumenteeritud**. Uute nõuete lisandumisel või olemasolevate nõuete muutumisel uuendatakse dokumentatsiooni.	Store; Update	event-based
161	E-ITS_2	CON.3.M2(a)	IT-talitus **koostab** andmevarunduse protseduure sisaldava andmevarunduseeskirja.	Store	one-off
162	E-ITS_2	CON.3.M4(a)	On **koostatud** andmevarundusplaanid erinevate andme- ja tarkvaratüüpide varundamiseks.	Store	one-off
163	E-ITS_2	CON.3.M6(a)	On **koostatud** andmevarunduse kontseptsioon, mis on kooskõlas organisatsiooni ärijätkuvusplaaniga (ingl business continuity plan, BCP) ja lubatava andmete kaoga peale taastamist (ingl recovery point objective, RPO)	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
164	E-ITS_2	CON.3.M9(a)	Välise salvestuskoha kasutamisel võrgustatud andmevarunduseks (ingl online backup) **sõlmitakse** teenusekvaliteedi tagamiseks teenusetasemelepe (ingl service level agreement, SLA) ja lepitakse kokku andmete füüsiline asukoht.	Store	event-based
165	E-ITS_2	CON.6.M1(a)	Organisatsioon on **kehtestanud** andmete kustutuse ja hävitamise korra	Store	one-off
166	E-ITS_2	CON.6.M8(a)	On **koostatud** andmete kustutuse ja hävitamise kirjalikud juhised, mis hõlmavad kõiki andmekandjaid, rakendusi, IT-süsteeme ja muid teavet sisaldada võivaid töövahendeid (nt nutiseadmed).	Store	one-off
167	E-ITS_2	CON.7.M1(a)	Infoturbe nõuded välisriigis viibimisel on **kehtestatud** välislähetuste infoturbe eeskirjas	Store	one-off
168	E-ITS_2	CON.7.M1(c)	Mobiilseid IT-seadmeid kasutavatele, välislähetustel käivatele töötajatele **koostatakse** infoturbe aspekte käsitlev teabeleht	Store	one-off
169	E-ITS_2	CON.7.M3(a)	Enne reisi algust tutvutakse riigikohaste õigusaktide ja kliimatingimustega ja **koostatakse** töötajatele vastav infomaterjal.	Store	event-based
170	E-ITS_2	CON.8.M3(a)	Enne tarkvaraarenduskeskkonna valimist on **dokumenteeritud** nõuded, millele tarkvaraarenduskeskkond ja -tööriistad peavad vastama ning määratud tööriistade valikukriteeriumid. Nõuded on kinnitanud tarkvaraarenduse eest vastutav töötaja.	Store	one-off
171	E-ITS_2	CON.8.M5(b)	Süsteemide kavandamise reeglid on **dokumenteeritud**. Tarkvaraarendajad on kehtestatud süsteemi kavandamise reeglitest teadlikud.	Store	one-off
172	E-ITS_2	CON.8.M11(a)	Organisatsioon on **kehtestanud** tarkvaraarenduste läbiviimise korra. Kord sisaldab antud moodulis käsitletud meetmeid, mis vastavad organisatsiooni spetsiifikale.	Store	one-off
173	E-ITS_2	CON.8.M12(a)	Tarkvaratoote kohta **on olemas** üksikasjalik ja põhjalik dokumentatsioon.	Store	one-off
174	E-ITS_2	CON.9.M2(a)	Organisatsioon on **kehtestanud** kõiki suulise ja elektroonilise teabevahetuse vorme hõlmava teabevahetuse korra	Store	one-off
175	E-ITS_2	CON.9.M2(b)	Organisatsioon on **kehtestanud** teabe kaitsetarbe määramise juhised ja kaitsetarbele vastavad meetmed teabe kaitsmiseks.	Store	one-off
176	E-ITS_2	CON.9.M9(a)	Konfidentsiaalse teabe edastuseks on selle saajaga **sõlmitud** leping, mis määrab: • milline teave on konfidentsiaalne ja kui kaua; • kellel on lubatud juurdepääs konfidentsiaalsele teabele; • kuidas konfidentsiaalset teavet on lubatud hoida; • millised on omandiõigused teabele ja saaja õigused teavet kasutada; • millised on konfidentsiaalsuslepingu rikkumise tagajärjed.	Store	one-off
177	E-ITS_2	CON.10.M1(d)	Kasutaja autentimisandmeid on lubatud veebirakenduses salvestada ainult pärast kaasnevate riskide kaalumist ja teadvustamist. Kasutajalt **nõutakse** enne oma autentimisandmete salvestamist riskidega tutvumist ja üheselt mõistetavat („opt-in") nõusolekut.	Collect	event-based
178	E-ITS_2	CON.10.M11(a)	Veebirakenduse tarkvaraarhitektuur koos kõikide komponentide ja sõltuvustega on **dokumenteeritud**. Tarkvaraarhitektuuri dokumentatsiooni uuendatakse ja kohandatakse vastavalt vajadusele.	Store; Update	one-off; event-based
179	E-ITS_2	OPS.1.1.1.M3(a)	Käitatavate IT-komponentide haldustööd **on kirjeldatud** IT-halduse juhendites	Store	one-off
180	E-ITS_2	OPS.1.1.1.M7(a)	IT-halduse protseduuridele on **kehtestatud** kvaliteedinõuded ning on määratud kriteeriumid IT-halduse toimingute nõuetele vastavuse mõõtmiseks.	Store	one-off
181	E-ITS_2	OPS.1.1.1.M7(d)	IT-halduse käigus tehtud tööd on sobival ja arusaadaval viisil **dokumenteeritud**. Soovitatav on kasutada selleks spetsiaalset tarkvara, nt IT Helpdeski rakendust.	Store	event-based
182	E-ITS_2	OPS.1.1.1.M9(a)	IT-komponentide seiret teostatakse keskse, IT-talituse juhtkonnas **kinnitatud** seireplaani alusel.	Store	one-off
183	E-ITS_2	OPS.1.1.1.M9(f)	IT-süsteemide kaetust IT-halduse seireplaaniga kontrollitakse perioodiliselt. IT-halduse seireplaani **ajakohastatakse** vastavalt vajadusele.	Update	event-based; periodic
184	E-ITS_2	OPS.1.1.1.M10(a)	IT-komponentide teadaolevad turvanõrkused **registreeritakse** keskses turvanõrkuste loendis	Store	event-based
185	E-ITS_2	OPS.1.1.1.M11(a)	IT-talitus on **sõlminud** oma klientidega IT-komponentide kaitsetarvet arvestavad teenusetasemelepped (ingl service level agreement, SLA) või tegevuslepped (ingl operational level agreement, OLA).	Store	event-based
186	E-ITS_2	OPS.1.1.1.M12(a)	IT-talitus on määratlenud ja **kinnitanud** IT-halduse protsessid.	Store	one-off
187	E-ITS_2	OPS.1.1.1.M12(d)	IT-halduse protsessi läbimise tõestusmaterjalid **dokumenteeritakse**. Üksikute protsessietappide läbimist logitakse vastavalt vajadusele.	Store	event-based
188	E-ITS_2	OPS.1.1.1.M12(e)	**On loodud** tegevusjuhised olukordadeks, mis väljuvad tüüpsete IT-halduse protsesside raamest. **Dokumenteeritud** on vähemalt: • tegevusjuhend juhuks, kui IT-halduse protsess ei ole võimalik; • juhised veaolukorra ja protsessi tahtliku manipuleerimise korral tegutsemiseks.	Store	one-off
189	E-ITS_2	OPS.1.1.1.M17(b)	IT-süsteemide pikaajalise katkestuse või avarii korral tegutsemiseks on **koostatud** IT-halduse avariiteatmik.	Store	one-off
190	E-ITS_2	OPS.1.1.1.M19(a)	IT-komponente hooldatakse regulaarselt. Teostatud hooldus- ja parendustööd **dokumenteeritakse**.	Store	event-based; periodic
191	E-ITS_2	OPS.1.1.1.M20(b)	IT-komponente testitakse turvanõrkuste olemasolu suhtes. Iga IT-komponendi jaoks on määratud sobiv testimise ulatus, sügavus ja metoodika. Testimisel tuvastatud turvanõrkused **registreeritakse**.	Store	event-based
192	E-ITS_2	OPS.1.1.2.M2(b)	Asendajate nimed ja kontaktandmed on **dokumenteeritud**	Store	one-off
193	E-ITS_2	OPS.1.1.2.M8(a)	Rakenduse- ja süsteemihaldurite vaheline ülesannete jaotus on määratletud ja **dokumenteeritud**.	Store	one-off
194	E-ITS_2	OPS.1.1.2.M11(a)	Kõik IT-süsteemi haldusega seotud muudatused **dokumenteeritakse**. Dokumentatsioonist on arusaadav, milliseid muudatusi ja millal on tehtud, kes muudatused tegi ning mis on muudatuse põhjus.	Store	event-based
195	E-ITS_2	OPS.1.1.2.M20(d)	Enne kasutuselevõttu läbivad seadmed kooskõlastusprotseduuri, mille käigus seadmed märgistatakse ja **registreeritakse** (nt varade registris)	Store	event-based
196	E-ITS_2	OPS.1.1.2.M29(a)	IT-süsteemide halduse tööriistadele on **kehtestatud** käideldavuse nõuded	Store	one-off
197	E-ITS_2	OPS.1.1.3.M1(a)	IT-komponentide, tarkvara ja konfiguratsiooniandmete muudatuste läbiviimiseks on **kehtestatud** paiga- ja muudatusehalduse kord	Store	one-off
198	E-ITS_2	OPS.1.1.3.M15(d)	Kui turvauuend otsustatakse mitte paigaldada, siis vastav otsus ja mittepaigaldamise põhjendus **dokumenteeritakse**.	Store	event-based
199	E-ITS_2	OPS.1.1.3.M5(a)	Muutmistaotlusi (inglise keeles Request for Changes, RfC) esitatakse, **registreeritakse ja dokumenteeritakse** vastavalt paiga- ja muudatusehalduse korrale.	Store	event-based

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
200	E-ITS_2	OPS.1.1.3.M8(b)	On **kehtestatud** paiga- ja muudatusehalduse tööriistade turvanõuded, mis käsitlevad tööriistade turvalist haldust ja logimise, andmevarunduse ning avariivalmenduse nõudeid.	Store	one-off
201	E-ITS_2	OPS.1.1.3.M9(c)	Riistvara testimistulemused ja kasutuselevõtuks kinnitamise tulemused **dokumenteeritakse**.	Store	event-based
202	E-ITS_2	OPS.1.1.3.M11(b)	Organisatsioonis on **kehtestatud** kord IT-süsteemides tehtud muudatuste dokumenteerimiseks.	Store	one-off
203	E-ITS_2	OPS.1.1.3.M13(c)	Järeltestimise tulemused **dokumenteeritakse**.	Store	event-based
204	E-ITS_2	OPS.1.1.4.M1(a)	On **koostatud** kontseptsioon, mis määrab, milliseid IT-süsteeme kahjurprogrammide eest kaitstakse ja kuidas	Store	one-off
205	E-ITS_2	OPS.1.1.4.M5(c)	Kui mõni toote turvafunktsioon on välja lülitatud, peab olema selleks **dokumenteeritud** põhjendus	Store	event-based
206	E-ITS_2	OPS.1.1.4.M9(d)	On **dokumenteeritud** ja testitud tegevuskava kahjurprogrammide eemaldamiseks ja nakatuseelse olukorra taastamiseks	Store	one-off
207	E-ITS_2	OPS.1.1.5.M1(a)	Organisatsioonis on **kehtestatud** infoturvapoliitikaga vastavuses olev logimise eeskiri, mis sätestab, kuidas logimist turvaliselt plaanida, korraldada ja rakendada	Store	one-off
208	E-ITS_2	OPS.1.1.5.M1(c)	Kõrvalekalded logimise eeskirjast kooskõlastatakse infoturbejuhiga ja **dokumenteeritakse**	Store	event-based
209	E-ITS_2	OPS.1.1.6.M3(b)	Testimistulemuste analüüsi tulemused **dokumenteeritakse**.	Store	event-based
210	E-ITS_2	OPS.1.1.6.M4(b)	Pärast edukat tarkvara testimist kinnitatakse tarkvara kasutuselevõtt **dokumenteeritud** otsusega	Store	one-off
211	E-ITS_2	OPS.1.1.6.M5(c)	Valitud testilood ja testimise tulemused **dokumenteeritakse**.	Store	event-based
212	E-ITS_2	OPS.1.1.6.M10(b)	On kehtestatud testimise vastuvõtu kord, mis määrab: • kohustuslikud testid; • oodatavad tulemused; • testimise vastuvõtu kriteeriumid.	Store	one-off
213	E-ITS_2	OPS.1.1.6.M12(b)	Valitud testimisjuhtumid ja testimistulemused **dokumenteeritakse**. Testimisjuhtumite väljajätmist põhjendatakse kirjalikult.	Store	event-based
214	E-ITS_2	OPS.1.1.6.M13(c)	Testkeskkonna arhitektuur ja tehnilised parameetrid on **dokumenteeritud**.	Store	one-off
215	E-ITS_2	OPS.1.1.6.M14(a)	On **koostatud** läbistustestimise (ingl penetration testing) juhend, mis määrab testimismeetodid ja tulemuskriteeriumid	Store	one-off
216	E-ITS_2	OPS.1.1.6.M14(c)	Läbistustestimise käigus tuvastatud nõrkused liigitatakse vastavalt riskiastmele ja **dokumenteeritakse**.	Store	event-based
217	E-ITS_2	OPS.1.1.7.M1(b)	On **kehtestatud** süsteemihalduse taristu tehnilised nõuded	Store	one-off
218	E-ITS_2	OPS.1.1.7.M2(a)	Süsteemihalduse lahenduse kavandamise tulemina on **dokumenteeritud**: • süsteemihalduse nõuete detailanalüüs; • süsteemihalduse lahenduse üldkontseptsioon; • terviklik projektiplaan süsteemihalduse lahenduse juurutamiseks; • projekti etappide lõpetamise eeldused ja läbiviidavad kvaliteedikontrollid.	Store	one-off
219	E-ITS_2	OPS.1.1.7.M6(c)	Kasutajate autentimise autentimismehhanismi valikuprotsess on **dokumenteeritud**.	Store	one-off
220	E-ITS_2	OPS.1.1.7.M7(a)	Süsteemihalduse turvalisuse tagamiseks on **koostatud** süsteemihalduse turvaeeskiri.	Store	one-off
221	E-ITS_2	OPS.1.1.7.M7(d)	Süsteemihalduse turvaeeskirja täitmist kontrollitakse regulaarselt. Kontrolli tulemused **dokumenteeritakse**.	Store	event-based; periodic
222	E-ITS_2	OPS.1.1.7.M8(a)	Organisatsioon on **koostanud** süsteemihalduse turvanõudeid (vt. OPS.1.1.7.M1 Süsteemihalduse nõuete määratlemine ja OPS.1.1.7.M7 Süsteemihalduse turvaeeskiri) arvestava süsteemihalduse kontseptsiooni.	Store	one-off
223	E-ITS_2	OPS.1.1.7.M9(a)	Süsteemihalduse lahenduse evitamiseks on **koostatud** detailne rakendusplaan, mis arvestab kõiki süsteemihalduse turvaeeskirjas ja kontseptsioonis sisalduvaid nõudeid.	Store	one-off
224	E-ITS_2	OPS.1.1.7.M10(a)	On **koostatud** juhised süsteemihalduse lahenduse turvaliseks käituseks	Store	one-off
225	E-ITS_2	OPS.1.1.7.M13(c)	Otsejuurdepääsu kasutamise juhud ning süsteemihalduse lahenduse väliselt tehtud konfiguratsioonimuudatused **dokumenteeritakse**. Tehtud muudatused kajastatakse hiljem süsteemihalduse lahenduses.	Store	event-based
226	E-ITS_2	OPS.1.1.7.M14(e)	Kõik liidesed süsteemihalduse lahenduse ning hallatavate IT-süsteemide vahel on **dokumenteeritud** keskses konfiguratsioonihalduse süsteemis. Seotud osapooled kooskõlastavad liideste funktsionaalsed muudatused enne muudatuste rakendamist	Store	one-off
227	E-ITS_2	OPS.1.2.2.M1(c)	On **koostatud** ja kinnitatud elektroonilise arhiveerimise konfidentsiaalsus-, terviklus-, käideldavus- ja autentsusnõuded.	Store	one-off
228	E-ITS_2	OPS.1.2.2.M2(a)	On **välja töötatud** arhiveerimiskontseptsioon, mis kirjeldab, milliseid eeskirju on vaja järgida, kes on vastutajad, milliseid andmeid ja millisel kujul tuleb arhiveerida ning millised on vajalikud turvameetmed.	Store	one-off
229	E-ITS_2	OPS.1.2.2.M10(a)	Organisatsioonis on **kehtestatud** arhiivisüsteemi kasutamise eeskiri, mis hõlmab järgnevat: • käituse ja halduse rollide lahusus ja vastutused; • kokkulepitud teenusetase; • pääsuõiguste haldus; • andmete ja andmekandjate käitluse protseduurid; • arhiivisüsteemi ja keskkonna järelevalve; • andmete varundamise protseduurid; • arhiivitoimingute logimine; • arhiivisüsteemi muudatuste haldus.	Store	one-off
230	E-ITS_2	OPS.1.2.2.M11(a)	Koolitus ja sellest osavõtt **dokumenteeritakse**.	Store	event-based
231	E-ITS_2	OPS.1.2.2.M15(b)	On **kehtestatud** turvaprotseduur krüptomehhanismi nõrgenemise puhuks (nt krüpteeritakse nõrgenenud krüptomehhanismiga arhiiviandmed uuesti, kasutades turvalisemat krüptoalgoritmi).	Store	one-off
232	E-ITS_2	OPS.1.2.2.M16(d)	Kõik arhiivisüsteemi komponentide muudatused, konverteerimised, testimised ja asenduskavad **dokumenteeritakse**.	Store; Update	event-based
233	E-ITS_2	OPS.1.2.2.M19(e)	Avastatud vigade ja ilmnenud tõrgete käsitluseks on **kehtestatud** protseduur.	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
234	E-ITS_2	OPS.1.2.4.M1(a)	Töötajatele järgimiseks on **koostatud** ja tehtud töötajatele kättesaadavaks kaugtöö korraldust reguleeriv eeskiri.	Store	one-off
235	E-ITS_2	OPS.1.2.4.M1(c)	On **koostatud** töökaitse õiguslikke aspekte arvestavad, tööandja ja töötaja vahelised kaugtöö kokkulepped, milles on määratletud vähemalt järgmine: • kaugtöö vabatahtlikkus; • töövahendid; • tööaeg ja kättesaadavus; • reageerimisajad, näiteks e-kirjade lugemise sagedus; • ületunnitöö, lisatasud ja täiendavate kulude tasumine; • materiaalne vastutus; • kaugtöö lõpetamine.	Store	one-off
236	E-ITS_2	OPS.1.2.4.M1(d)	Kaugtöö eeskirja vaadatakse üle ja seda ajakohastatakse regulaarselt.	Store; Update	periodic
237	E-ITS_2	OPS.1.2.4.M6(a)	On **koostatud** kaugtöö turbekontseptsioon, mis esitab kaugtöökoha kaitsetarbe, turvaeesmärgid ja turvanõuded.	Store	one-off
238	E-ITS_2	OPS.1.2.4.M6(d)	Kontseptsiooni **ajakohastatakse** regulaarselt.	Update	periodic
239	E-ITS_2	OPS.1.2.4.M10(a)	Enne kaugtöökohtade loomist on **läbi viidud** nõuete analüüs, mis sisaldab vähemalt järgmist: • konfidentsiaalsusnõuded kaugtöökohas käideldavale teabele; • organisatsioonile juurdepääsu saamise eesmärgid; • andmeliikluse maht kaugtöökoha ja organisatsiooni vahel; • sisevõrguteenuste kasutamise vajadused; • Interneti kasutamise vajadused; • nõuded dokumentide ja andmekandjate transportimisele: • kaugtöökoha riist- ja tarkvarakomponentide vajadus ja valik (kooskõlastatakse IT-haldusega).	Store	event-based
240	E-ITS_2	OPS.1.2.4.M10(b)	Konkreetse kaugtöökoha nõuded **dokumenteeritakse** ja kooskõlastatakse IT-juhiga.	Store	event-based
241	E-ITS_2	OPS.1.2.5.M17(b)	Autentimismeetodi valik ja selle valimise põhjused on **dokumenteeritud**	Store	event-based
242	E-ITS_2	OPS.1.2.5.M19(a)	Kõik välise teenuseandja poolt kaughooldusena tehtud muudatused (nt konfigureerimisseadetes, lähtekoodis) **dokumenteeritakse**. Muudatuste dokumentatsioon antakse üle kaughooldatavale organisatsioonile.	Store; Update	event-based
243	E-ITS_2	OPS.2.2.M1(a)	On **kehtestatud** pilvteenuste strateegia, mis on kooskõlas organisatsiooni eesmärkidega ja kus on dokumenteeritud: • pilvteenuste eesmärgid, eelised ja riskid; • pilvteenuste kasutamisega seotud õiguslikud, korralduslikud, majanduslikud ja tehnilised raamtingimused; • eeldatavad pilvteenused ja nende kasutusviisid; • mõjutatud äriprotsesside säilenõtkuse (ingl resilience) tagamine pilvteenuste lõpetamisel.	Store	one-off
244	E-ITS_2	OPS.2.2.M1(c)	Iga kavandatava pilvteenuse kohta **viiakse läbi** teostatavuse, tasuvuse ja turvalisuse analüüs.	Store	event-based
245	E-ITS_2	OPS.2.2.M1(d)	Pilvteenuste kasutuselevõtuks **koostatakse** etapiviisiline teenuse kasutuselevõtu plaan	Store	one-off
246	E-ITS_2	OPS.2.2.M2(a)	Pilvteenuste strateegiast (vt OPS.2.2.M1 Pilvteenuste strateegia) lähtuvalt on **koostatud** pilvteenuste turvapoliitika	Store	one-off
247	E-ITS_2	OPS.2.2.M3(a)	Kõik kavandatavad ja kasutatavad pilvteenused **dokumenteeritakse** ühtsetel alustel.	Store	event-based
248	E-ITS_2	OPS.2.2.M4(a)	Määratletakse ja **dokumenteeritakse** pilvteenuse kasutamisega seotud vastutusalad ja teenusepoolte tegevused.	Store	event-based
249	E-ITS_2	OPS.2.2.M4(b)	Valitakse ja **dokumenteeritakse** pilvteenuse rakenduseks vajalikud IT-komponendid (nt. andmete varundussüsteem) ning riist- ja tarkvaraline liidestus.	Store	event-based
250	E-ITS_2	OPS.2.2.M5(a)	Pilvteenusele siirdumiseks **koostatakse** pilvteenusele migreerimise kava, mis määrab: • rollid ja kohustused; • IT-keskkonna ja käiduprotseduuride ettevalmistuse; • testimis- ja üleviimisprotseduurid; • teenusetaseme ja turvataseme vastavuskontrolli; • pilvteenusest loobumise protseduurid.	Store	one-off
251	E-ITS_2	OPS.2.2.M6(b)	Pilvteenusega liitumise tegevusplaan on **dokumenteeritud**, tegevusplaani uuendatakse regulaarselt.	Store; Update	periodic
252	E-ITS_2	OPS.2.2.M8(a)	Pilvteenuse andja valimiseks **koostatakse** pilvteenuste loendi (vt OPS.2.2.M3 Pilvteenuste loendi koostamine) andmeid sisaldav ja neid täiendav nõuete spetsifikatsioon.	Store	one-off
253	E-ITS_2	OPS.2.2.M14(a)	Pilvteenuselepingu lõppemise puhuks on **kehtestatud** protseduurid üleminekuks sisemisele teenusele või teisele pilvteenuseandjale, täites kõiki seniseid teenusenõudeid.	Store	one-off
254	E-ITS_2	OPS.2.3.M1(a)	Kõikidele väljasttellitavatele teenustele on **kehtestatud** kaitsetarbe määramisele ja/või ärimõjude hindamisele (ingl business impact assessment, BIA) põhinevad turvanõuded	Store	one-off
255	E-ITS_2	OPS.2.3.M3(a)	Teenuseandja valimiseks on **koostatud** turvanõudeid sisaldav nõuete profiil	Store	one-off
256	E-ITS_2	OPS.2.3.M4(a)	Kõik väljasttellitava teenuse aspektid **lepitakse** teenuseandjaga **kirjalikult kokku** teenuselepingus. Teenuselepingute tarbeks on loodud ühtne lepinguvorm.	Store	event-based
257	E-ITS_2	OPS.2.3.M8(a)	Organisatsioonis on **kehtestatud** majanduslikke, tehnilisi, korralduslikke ja õiguslikke raamtingimusi ning infoturbe aspekte käsitlev väljasttellimise strateegia.	Store	one-off
258	E-ITS_2	OPS.2.3.M9(a)	Väljasttellimise strateegiast (vt OPS.2.3.M8 Väljasttellimise strateegia) lähtudes on **koostatud** ja kinnitatud organisatsiooni hankepoliitika	Store	one-off
259	E-ITS_2	OPS.2.3.M11(a)	Väljasttellimise eest vastutaja **koondab** allhankeid käsitleva dokumentatsiooni väljasttellitud teenuste registrisse	Store	event-based
260	E-ITS_2	OPS.2.3.M12(a)	Väljasttellimise eest vastutaja **koostab** juhtkonnale perioodiliselt aruandeid teenuse hetkeseisust ja võimalikest kitsaskohtadest	Store	periodic
261	E-ITS_2	OPS.2.3.M15(a)	Enne teenuseandja kliendi võrku lubamist on kokku lepitud ja **dokumenteeritud**: • ühenduse kasutamise korralduslikud ja tehnilised tingimused; • ühenduse kaitsetarve ja turvameetmed; • poolte konfidentsiaalsuskohustused; • eritingimused välismaise teenuseandja puhul.	Store	event-based
262	E-ITS_2	OPS.2.3.M16(b)	Teenuseandja infoturbe läbivaatuste tulemused **dokumenteeritakse**.	Store	event-based
263	E-ITS_2	OPS.3.2.M2(a)	Teenuseandja on **välja töötanud** tüüptingimusi sisaldavad teenuselepingu vormid.	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
264	E-ITS_2	OPS.3.2.M5(a)	Teenuseandja on **koostanud** kõiki klientidele pakutavaid teenuseid hõlmava turvakontseptsiooni.	Store	one-off
265	E-ITS_2	OPS.3.2.M6(e)	Kui ei ole teisiti kokku lepitud, kustutatakse teenuseandja juures edasi hoiustatavad kliendi andmed turvaliselt pärast seadusest tuleneva säilitustähtaja täitumist. Andmete kustutamise fakt **dokumenteeritakse**.	Store	event-based
266	E-ITS_2	OPS.3.2.M7(a)	Allhankijate teenuseid kasutav teenuseandja on **koostanud** alternatiivsete allhankijate loendi	Store	one-off
267	E-ITS_2	OPS.3.2.M8(a)	Teenuseandja on **dokumenteerinud** põhimõtted teenuste loomiseks, testimiseks ja kasutusele võtuks.	Store	one-off
268	E-ITS_2	OPS.3.2.M10(b)	Teenuseandja ja klient on kokku leppinud ja **dokumenteerinud**, millist teavet suhtluspartnerite vahel edastatakse ning kes on poolte kontaktisikud.	Store	one-off
269	E-ITS_2	OPS.3.2.M12(b)	Riskianalüüsi tulemid **dokumenteeritakse** ja neid kasutatakse infoturbe edasiseks täiustamiseks.	Store	event-based
270	E-ITS_2	OPS.3.2.M13(a)	Enne andmevahetuse alustamist lepitakse kokku ja **dokumenteeritakse**: • kasutatavad rakendused; • kasutatavad andmevormingud; • andmete käideldavuskriteeriumid (siinhulgas päringutele reageerimise aeg); • teabevahetuse turbe meetmed (vt CON.9 Teabevahetus); • turvamehhanismid (viirusetõrje, krüpteerimine, signeerimine, võtmehaldus jms).	Store	one-off
271	E-ITS_2	OPS.3.2.M16(a)	Teenuseandja on **dokumenteerinud** allhankijate osalusega protsessid, peamised tulemusnäitajad, teenuse osutamisega seotud allhankijad ja nendega sõlmitud lepingud.	Store	one-off
272	E-ITS_2	DER.1.M1(a)	Organisatsiooni üldisest turvapoliitikast lähtudes on **koostatud** eeskiri, milles on kirjeldatud turvaintsidentide õigeaegseks avastamiseks vajalikud plaanimis- ja operatiivtegevused.	Store	one-off
273	E-ITS_2	DER.1.M1(c)	Turvaintsidentide avastamise eeskirja järgimist kontrollitakse regulaarselt, kontrolli tulemused **dokumenteeritakse**	Store	event-based; periodic
274	E-ITS_2	DER.1.M2(a)	Logiandmete analüüsiks on **koostatud** juhend, milles on esitatud kohaldatavad õigusaktide nõuded. Juhendit ajakohastatakse õiguslike raamtingimuste muutumisel.	Store; Update	event-based
275	E-ITS_2	DER.1.M3(a)	Organisatsioonis on **kehtestatud** turvasündmustest teavitamise kord, kus dokumenteeritakse teavitusteed ja adressaadid eri liiki intsidentide puhuks, teavitatavad isikud, isikute kättesaadavus ja intsidendi kiireloomulisusest sõltuv sidekanali valik.	Store	one-off
276	E-ITS_2	DER.1.M6(b)	Turvaintsidentide avastamiseks on **koostatud** IT-süsteemide põhised logiandmete analüüsi juhised	Store	one-off
277	E-ITS_2	DER.1.M13(b)	Läbivaatuse tulemused **dokumenteeritakse** ja neid võrreldakse eelmiste läbivaatuste tulemustega. Kõrvalekaldeid kontrollitakse.	Store	event-based
278	E-ITS_2	DER.2.1.M2(a)	Turvaintsidentide käsitluseks on **koostatud** protseduurijuhend. Juhendis on määratud käsitlusala, millele juhend laieneb.	Store	one-off
279	E-ITS_2	DER.2.1.M5(a)	Turvaintsidendi lahendamiseks isoleeritakse mõjutatud komponendid, intsident **dokumenteeritakse** ja selgitatakse välja selle põhjus.	Store	event-based
280	E-ITS_2	DER.2.1.M7(c)	Turvaintsidentide käsitluse metoodikat kontrollitakse ja **ajakohastatakse** regulaarselt.	Update	periodic
281	E-ITS_2	DER.2.1.M9(a)	Intsidentidest teavitamiseks koostatakse **juhend**, mis sätestab vähemalt järgmist: • lubatavad ja sobivad teavitusteed eri liiki intsidentide puhuks; • isikute nimekiri, keda informeeritakse kindlasti ja keda vajadusel; • kelle kaudu, millises järjekorras ja millise täpsusega teave liigub; • kes edastab turvaintsidentidega seotud teavet kolmandatele pooltele.	Store	one-off
282	E-ITS_2	DER.2.1.M10(b)	Kõige tõenäolisemate intsidendistsenaariumide jaoks on **koostatud** intsidendi käsitlemise tegevuskava.	Store	one-off
283	E-ITS_2	DER.2.1.M11(a)	Turbehalduse ja intsidendihalduse funktsioonidele on **kehtestatud** turvaintsidentide ja muude häiringute (nt IT-rikete) hindamiseks ja liigitamiseks ühtne protseduur.	Store	one-off
284	E-ITS_2	DER.2.1.M14(a)	Lisaks kommunikatsiooniplaanile (vt DER.2.1.M9 Turvaintsidentidest teavitamise juhend) **luuakse** turvaintsidentidest teavitamise eskalatsiooniplaan, mis kooskõlastatakse infoturbejuhiga.	Store	one-off
285	E-ITS_2	DER.2.2.M5(a)	On **koostatud** asitõendite turbe juhend, mis sisaldab meetodeid, tehnilisi vahendeid, õiguslikke raamtingimusi ja dokumenteerimisnõuded asitõendite tõendusväärtuse tagamiseks.	Store	one-off
286	E-ITS_2	DER.2.2.M8(b)	Asitõendite kogumiseks ja turbeks **koostatakse** tegevuskava. Tegevuste järjestamisel lähtutakse asitõendite volatiilsusest.	Store	event-based
287	E-ITS_2	DER.2.2.M11(a)	Kriminalistikauuringu käigus **dokumenteeritakse** kõik läbiviidud sammud, kasutatud meetodid, kasutamise põhjused ja läbiviimise eest vastutajad.	Store	event-based
288	E-ITS_2	DER.2.2.M13(a)	Infoturvaintsidentide kriminalistikauuringu kiiremaks käivitamiseks on organisatsioon **sõlminud** kriminalistikateenuse tarnijatega kaasamislepped või raamlepingud.	Store	one-off
289	E-ITS_2	DER.2.2.M14(a)	Suure kaitsetarbega rakenduste, IT-süsteemide ja enamlevinud süsteemikonfiguratsioonide terviklikuks salvestamiseks on **koostatud** kriminalistikanõuetele vastavad tüüpprotseduurid. Protseduurid arvestavad nii volatiilseid kui vähemuutuvaid andmeid.	Store	one-off
290	E-ITS_2	DER.3.1.M13(c)	Dokumentide ülevaatuse tulemused **dokumenteeritakse**. Tulemusi arvestatakse kohapealsete kontrollide läbiviimisel.	Store	event-based
291	E-ITS_2	DER.3.1.M14(a)	Kohapealse kontrolli osana tehtavad pistelised kontrollid valitakse riskipõhiselt, valikud **dokumenteeritakse** ja põhjendatakse.	Store	event-based
292	E-ITS_2	DER.3.1.M2(a)	Auditi või läbivaatuse kavandamisel lepitakse kokku ja **dokumenteeritakse** auditi või läbivaatuse käsitlusala ja eesmärgid.	Store	event-based
293	E-ITS_2	DER.3.1.M3(e)	Auditi või läbivaatuse tulemused **dokumenteeritakse** ühtsel, eelnevalt kokkulepitud kujul	Store	event-based
294	E-ITS_2	DER.3.1.M6(b)	Meetmete rakendamise hindamiseks on kehtestatud ja **dokumenteeritud** ühtne hindamissüsteem	Store	one-off
295	E-ITS_2	DER.3.1.M7(a)	Organisatsioon **koostab** mitmeaastast perioodi hõlmava auditite ja läbivaatuste kava.	Store	periodic
296	E-ITS_2	DER.3.1.M10(a)	Enne auditi algust **koostab** auditijuht auditiplaani, mis võetakse auditi läbiviimise aluseks	Store	one-off
297	E-ITS_2	DER.3.1.M22(a)	Auditirühm **dokumenteerib** auditi tulemused arusaadavalt ja põhjalikult ning **esitab** need auditi aruandena. Auditirühm on valmis vajadusel audititulemusi selgitama.	Store	event-based
298	E-ITS_2	DER.3.2.M2(a)	Organisatsioonis on **koostatud** ja juhtkonnas kinnitatud auditite läbiviimise juhend, milles esitatakse auditi eesmärgid, vastavusnõuded ning teave auditi tellimise, korralduse ja ressursside kohta	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
299	E-ITS_2	DER.3.2.M4(c)	Juhtaudiitor **koostab** kogu audititsüklit hõlmava auditikava, mille põhjal täpsustatakse ja kinnitatakse igal aastal infoturbe auditite aastaplaan	Store	periodic
300	E-ITS_2	DER.4.M1(a)	Organisatsioon on koostanud avarii korral tegutsemise juhiseid sisaldava avariiteatmiku, milles on esitatud vähemalt: • kaasatud rollid, töötajate õigused ja kohustused; • kiirjuhised töötajatele; • alarmeerimine ja käsitluse laiendamine; • teabevahetuse, jätkusuutlikkuse tagamise ja taaskäivituse korrad; • IT-süsteemide taasteplaanid.	Store	one-off
301	E-ITS_2	DER.4.M3(a)	Avariihalduse käsitlusala ja strateegia **kehtestatakse** organisatsiooni juhtkonnas vastavalt organisatsiooni eesmärkidele ja jääkriskide tasemele.	Store	one-off
302	E-ITS_2	DER.4.M4(a)	Organisatsiooni juhtkond on **kinnitanud** avariihalduse poliitika.	Store	one-off
303	E-ITS_2	DER.4.M8(a)	Töötajate regulaarseks teavitamiseks on **koostatud** rollipõhine avariihalduse teadvustus- ja koolituskava.	Store	periodic
304	E-ITS_2	DER.4.M10(a)	On **koostatud** õppuste plaan, mille kohaselt regulaarselt ja juhtumipõhiselt testitakse ja harjutatakse olulisemaid avariihalduse tegevuskavasid ja meetmeid.	Store	one-off
305	E-ITS_2	DER.4.M12(a)	Avariihalduse toimingud, vahetulemused ja olulised otsused **dokumenteeritakse**	Store	event-based
306	E-ITS_2	DER.4.M15(b)	Hindamistulemustest teavitatakse juhtkonda, kes otsustab avariihalduse täiustamise. Juhtkonna otsused **dokumenteeritakse**.	Store; Provide	event-based
307	E-ITS_2	INF.1.M5(d)	Käsikustuteid kontrollitakse ja hooldatakse regulaarselt, kontrollimisaeg ja hooldusvälp on **dokumenteeritud**.	Store	periodic
308	E-ITS_2	INF.1.M9(a)	Organisatsiooni üldise turbekontseptsiooni alusel on **kehtestatud** hoonete turbe programm, mis sätestab muuhulgas: • suure kaitsetarbega ruumide paigutuse põhimõtted; • ruumidesse pääsu reguleerimise; • valvesüsteemide kasutamise; • vee- ja tuleõnnetuste mõju vähendamise meetmed; • hoone asukohast tulenevad lisameetmed; • IT-taristu tulekaitse meetmed; • tehnoteenuste turbe.	Store	one-off
309	E-ITS_2	INF.1.M12(b)	Pääsmikke ja võtmeid väljastatakse ainult põhjendatud juhtudel ja volitatud isikutele, väljastused ja tagastused **dokumenteeritakse**.	Store	event-based
310	E-ITS_2	INF.1.M14(a)	Hoone piksekaitsesüsteemi kaitseklassi valikul on lähtutud asjakohase standardi alusel **koostatud** riskianalüüsi tulemustest (standardid EN 62305, EVS-HD 60364 ja EVS-EN 60099).	Store	one-off
311	E-ITS_2	INF.1.M15(d)	Juhistike ja torustike hooldustööd on **dokumenteeritud**.	Store	event-based
312	E-ITS_2	INF.1.M20(a)	Tuleohu korral tegutsemiseks on **koostatud** tulekahju korral tegutsemise plaan.	Store	one-off
313	E-ITS_2	INF.1.M23(d)	Hoonete ja territooriumi turvatsoonid ja nende kaitsetarve on **dokumenteeritud**	Store	one-off
314	E-ITS_2	INF.1.M26(a)	Valve- ja turvateenistuse ülesanded on selgelt dokumenteeritud.	Store	one-off
315	E-ITS_2	INF.2.M1(a)	Andmekeskuse või serveriruumi tarbeks on **kehtestatud** tehnilised ja korralduslikud nõuded.	Store	one-off
316	E-ITS_2	INF.2.M6(c)	Kõik sisenemised andmekeskusesse **registreeritakse**.	Store	event-based
317	E-ITS_2	INF.2.M10(b)	Taristu ülevaatused ja hooldetööd **dokumenteeritakse**.	Store	event-based
318	E-ITS_2	INF.2.M29(c)	Kui andmekeskust või serveriruumi läbib muid juhtmeid, on nende kasutamise põhjus **dokumenteeritud**. Ka neid juhtmeid käsitletakse ja kaitstakse andmekeskuses kehtivate nõuete kohaselt.	Store	one-off
319	E-ITS_2	INF.2.M14(e)	Generaatori kütusemahuti tankimised **dokumenteeritakse**.	Store	event-based
320	E-ITS_2	INF.2.M19(b)	Taristu testimise tulemused **dokumenteeritakse**.	Store	event-based
321	E-ITS_2	INF.5.M3(c)	Kõik tehnilise taristu ruumis viibimised **registreeritakse**	Store	event-based
322	E-ITS_2	INF.5.M17	Taristu ülevaatused ja hooldetööd **dokumenteeritakse**	Store	event-based
323	E-ITS_2	INF.6.M7(c)	Õhutemperatuuri ja -niiskuse näidud **registreeritakse**. Kõrvalekalletele reageeritakse koheselt	Store	event-based
324	E-ITS_2	INF.7.M5(d)	Arvutiga töötajatele on **kehtestatud** kuvariga töötamise kord, mis sätestab regulaarsete puhkepauside tegemise.	Store	one-off
325	E-ITS_2	INF.8.M2(a)	On **kehtestatud** organisatsiooni dokumentide ja andmekandjate käitlemise kord, mis määrab: • milliseid materjale ja millisel viisil on lubatud transportida (post, kuller vm); • milliseid turvameetmeid rakendatakse transpordil (sobiv pakend, märgistus vm); • milliseid materjale on lubatud transportida ainult personaalselt; • milliseid andmeid enne transportimist varundatakse.	Store	one-off
326	E-ITS_2	INF.8.M5(a)	Konfidentsiaalsete andmete kõrvaldamiseks on **kehtestatud** kord. Andmete kõrvaldamisel kodutöökohal järgitakse organisatsioonis selleks kehtestatud korda.	Store	one-off
327	E-ITS_2	INF.9.M1(a)	Organisatsioon on **kehtestanud** nõuded, millele mobiiltöökoht peab vastama.	Store	one-off
328	E-ITS_2	INF.9.M4(a)	On **kehtestatud** kord organisatsioonivälistе IT-süsteemide (internetikohvik, külastatava ettevõtte kontoriarvuti vms) tööalaseks kasutamiseks.	Store	one-off
329	E-ITS_2	INF.9.M8(a)	Üldise turvapoliitika alusel on **kehtestatud** mobiiltöökoha turvaeeskiri või täiendatud mobiiltöökoha turvanõuetega mobiilseadme kasutamise eeskirja (vt INF.9.M1 Mobiilseadmete kasutamise eeskiri).	Store	one-off
330	E-ITS_2	INF.10.M1(a)	On kehtestatud ja dokumenteeritud ruumi kasutamise kord, mis määrab: • kes haldab ruumis asuvaid IT- ja muid süsteeme; • millistel tingimustel tohivad külastajad kasutada kaasatoodud IT-vahendeid; • milliseid võrguühendusi ja -liideseid tohivad külastajad kasutada.	Store	one-off
331	E-ITS_2	INF.10.M8(b)	Organisatsioonis on **rakendatud** kord ja protseduurid koosoleku-, ürituse- ja koolitusruumide eelnevaks reserveerimiseks.	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
332	E-ITS_2	INF.11.M3(a)	Sõidukis töödeldavad andmed (sh isikuandmed) on kaardistatud ja **dokumenteeritud**.	Store	one-off
333	E-ITS_2	INF.11.M3(e)	On **koostatud** juhendid sõiduki IT-süsteemide turvaliseks kasutamiseks ja haldamiseks.	Store	one-off
334	E-ITS_2	INF.11.M4(b)	Sõidukite infoturbe eeskiri on **dokumenteeritud**, asjaomastele töötajad järgivad kinnitatud sõidukite infoturbe eeskirja	Store	one-off
335	E-ITS_2	INF.11.M5(a)	Sõiduki kohta on **koostatud** loend sõidukisse täiendavalt lisatud IT-komponentidest ja seadmetest (nt käsiraadiojaam).	Store	one-off
336	E-ITS_2	INF.11.M6(a)	On **koostatud** detailsed tegevusjuhised tegutsemiseks sõiduki avariiolukorra ja IT-komponentide rikke korral.	Store	one-off
337	E-ITS_2	INF.11.M6(c)	On **koostatud** tegevusjuhend tegutsemiseks sõiduki ärandamise või volitamata sissetungi puhuks	Store	one-off
338	E-ITS_2	INF.11.M7(a)	Organisatsioon on **kehtestanud** sõidukite kasutamise korra, mis määratleb: • kes ja mis otstarbel võivad sõidukit kasutada; • kuidas on korraldatud sõiduki parkimine; • vargusvastased vahendid, mis tuleb sõiduki parkimisel (või veesõiduki dokkimisel) aktiveerida; • sõidukis viibivate inimeste ja veose kaitsemeetmed.	Store	one-off
339	E-ITS_2	INF.11.M11(a)	Organisatsioon on **koostanud** tegevuskava juhuks kui sõidukit tabab ootamatu tehniline rike või muu asjaolu, miks sõidukit antud hetkel ei ole võimalik kasutada.	Store	one-off
340	E-ITS_2	INF.12.M1(e)	Sidekaabli liigi (koaksiaal-, keerdpaar-, valguskaabel) ja kaablitüübi valiku põhjendused on **dokumenteeritud**.	Store	event-based
341	E-ITS_2	INF.12.M2(a)	Enne kaablite valimist ja paigaldust on **koostatud** elektri- ja sidekaabelduse kava, millega on määratud kaablite turvaline paigutus, jaotuspunktid, läbiviigud ja reservivajadus.	Store	event-based
342	E-ITS_2	INF.12.M10(a)	Kaabelduse **dokumentatsioon** sisaldab kaabliskeeme, hooneplaane, rennide asendiplaane, pistikupesade asukohti ja jaotuskappide kaabliühendusjooniseid.	Store	one-off
343	E-ITS_2	INF.12.M13(b)	Isiklike elektriseadmete kasutamine on reguleeritud ja toimub selleks **kehtestatud** korra alusel.	Store	one-off
344	E-ITS_2	INF.12.M5(b)	Sidekaabelduse kavandamisel on kaablite liigi ja konstruktsiooni valimiseks tehtud nõuete analüüs, milles on võetud arvesse: • lähiperspektiivis vajalik läbilaskevõime; • läbilaskevõime vajaduse kasv tulevaste teenuste ja rakenduste lisandumise tõttu; • andmeedastuse käideldavus, terviklus ja konfidentsiaalsus; • erinevad kaablid teatud rakendustele (nt valvesüsteem, protsessijuhtimine); • eraldi kaablid teiste vajadustega või erineva kaitsetarbega aladele; • aktiivkomponentide toitevajadus sidekaablist; • lahenduse maksumus.	Store	event-based
345	E-ITS_2	INF.12.M6(a)	Kaabelduse vastuvõtmiseks on **kehtestatud** ja **dokumenteeritud** protseduur ja kontroll-loend.	Store	one-off
346	E-ITS_2	INF.12.M6(d)	Vastuvõtu kontroll-loend ja kõikide osapoolte siduvalt allkirjastatud üleandmis-vastuvõtuakt **säilitatakse** osana kaabelduse sisedokumentatsioonist.	Store	one-off
347	E-ITS_2	INF.12.M8(d)	On olemas ajakohane **ülevaade**, millised kaablid seisavad kasutuseta, on lahti ühendatud või eemaldatud. Muudatused kaabelduses dokumenteeritakse.	Store; Update	event-based
348	E-ITS_2	INF.12.M12(d)	Testimise ja visuaalse ülevaatuse käigus avastatud puudused **dokumenteeritakse** ja edastatakse vastutajatele puuduste kõrvaldamiseks ja põhjuste väljaselgitamiseks.	Store	event-based
349	E-ITS_2	INF.13.M2(a)	Kuna erinevad hoone tehnilise halduse valdkonnad vajavad erinevaid oskusi, on määratletud ja **dokumenteeritud** iga valdkonna protsessidega seotud õigused, kohustused ja tööülesanded.	Store	one-off
350	E-ITS_2	INF.13.M2(d)	Kõigi hoone tehnilises halduses osalejate vahel on kokku lepitud ja **dokumenteeritud** andmevahetus-, aruandlus- ja suhtluskanalid.	Store	one-off
351	E-ITS_2	INF.13.M4(a)	Organisatsioon on **kehtestanud** üldise turvapoliitikaga kooskõlas oleva hoonete tehnilise halduse turvaeeskirja	Store	one-off
352	E-ITS_2	INF.13.M6(a)	Hoone tehnilise halduse kavandamine ja turvanõuded on **koondatud** hoonete tehnilise halduse kontseptsiooni.	Store	one-off
353	E-ITS_2	INF.13.M6(c)	Hoonete tehnilise halduse kontseptsiooni valideeritakse ja vajadusel **uuendatakse** regulaarselt.	Update	periodic; one-off; event-based
354	E-ITS_2	INF.13.M6(e)	Ülevaatuste tulemused **dokumenteeritakse**, võimalike kõrvalekalletega tegeletakse esimesel võimalusel.	Store	event-based
355	E-ITS_2	INF.13.M7(a)	Kõik traadita andmesidet (sh WLAN, Bluetooth ja mobiilne andmeside) kasutavad tehnosüsteemid on organisatsiooni erinevate asukohtade lõikes kaardistatud. Erinevad sagedusalad ja nende kasutajad on **lisatud** raadiosageduste loendisse.	Store	periodic
356	E-ITS_2	INF.13.M8(a)	Hoone tehnilise halduse süsteemi komponendid on kaardistatud ja **kantud** hoone tehnilise halduse objektide loendisse.	Store	event-based
357	E-ITS_2	INF.13.M11(a)	Hoonete tehnilise halduse (ingl Technical Building Management, TBM) protsessi infoturbe tugevdamise (ingl hardening) meetmed on **dokumenteeritud**.	Store	one-off
358	E-ITS_2	INF.13.M14(d)	Tehniliste kasutajate rollid (st rollid seadmevaheliseks andmevahetuseks) on **dokumenteeritud**. Tarbetud tehnilised kasutajad on desaktiveeritud.	Store	one-off
359	E-ITS_2	INF.13.M16(b)	On **koostatud** juhend juhuks, kui ebaõnnestunult läbiviidud muudatust ei ole võimalik tagasi pöörata või kui endise olukorra taastamine on tehtav ainult suurte jõupingutustega.	Store	one-off
360	E-ITS_2	INF.13.M17(a)	Hoonete regulaarsete hoolduste läbiviimiseks on **koostatud** hooldusplaan, mis muuhulgas sisaldab ka hooldus- ja remonditööde turvaaspekte.	Store	one-off
361	E-ITS_2	INF.13.M17(d)	Hoonetes tehtud hooldus- ja remonditööd on **dokumenteeritud**.	Store	event-based
362	E-ITS_2	INF.13.M26(a)	Kui hooneteabe digitaalse modelleerimise tarkvara (ingl Building Information Modeling, BIM) sisaldab turvalisuse seisukohast olulist teavet, on BIM arhitektuurile, BIM juurutamisele ja käitamisele **kehtestatud** täiendavad turvameetmed.	Store	one-off
363	E-ITS_2	INF.13.M28(a)	Intellektitehnikat (ingl artificial intelligence, AI) kasutavad komponendid, nende funktsionaalsus ja toimepõhimõtted on **dokumenteeritud**.	Store	event-based
364	E-ITS_2	INF.14.M2(c)	Hooneautomaatikasüsteemi andmevahetusliidesed on **dokumenteeritud**	Store	one-off
365	E-ITS_2	INF.14.M5(a)	Kõigi kasutatavate hooneautomaatikasüsteemi komponentide (sh tehnosüsteemid ja taristukomponendid) kasutamine, juurdepääs, omavahelised sõltuvused ja andmeliidesed on **dokumenteeritud**.	Store	event-based

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
366	E-ITS_2	INF.14.M7(a)	Lähtudes üldise turvapoliitikast ja hoonete tehnilise halduse turvanõuetest (INF.13.M4 Hoonete tehnilise halduse turvaeeskiri) on **koostatud** hooneautomaatikasüsteemi turvaeeskiri.	Store	one-off
367	E-ITS_2	INF.14.M8(a)	Hooneautomaatikasüsteemi turvaeeskirja (vt INF.14.M7 Hooneautomaatikasüsteemide turvaeeskiri) alusel on **koostatud** iga hooneautomaatikasüsteemi jaoks nõuete spetsifikatsioon. Nõuete spetsifikatsiooni koostamisel on arvestatud ka hoone arhitektuurist ja organisatsiooni äriprotsessidest tulenevaid erinõudeid.	Store	one-off
368	E-ITS_2	INF.14.M9(a)	Organisatsioonis on **välja töötatud** hooneautomaatikasüsteemide turvaeeskirjal ning nõuete spetsifikatsioonil põhinev üldine hooneautomaatikasüsteemi kontseptsioon.	Store	one-off
369	E-ITS_2	INF.14.M13(c)	Võrgu segmentimine on põhjalikult **dokumenteeritud**	Store	event-based
370	E-ITS_2	INF.14.M27(c)	Hooneautomaatikasüsteemi avarii korral käitumiseks on **koostatud** hooneautomaatikasüsteemi avariihalduse tegevuskava (vt DER.4 Avariihaldus).	Store	one-off
371	E-ITS_2	INF.14.M27(f)	Hooneautomaatikasüsteemi oluliste komponentide töö taastamiseks pärast avariid on **koostatud** taasteplaanid.	Store	one-off
372	E-ITS_2	NET.1.1.M1(a)	Võrgu turvapoliitika on **kehtestatud** lähtuvalt üldisest infoturvapoliitikast. Võrgu turvapoliitika esitab nõuded ja juhised võrgu turvaliseks kavandamiseks ja teostuseks.	Store	one-off
373	E-ITS_2	NET.1.1.M2(a)	Võrgulahendus on **dokumenteeritud** ja sisaldab vähemalt järgmist: • võrgu loogilist ülesehitust esitavat võrguskeemi; • alamvõrkude, tsoonide ja segmentide kirjeldust; • võrgus tehtud muudatusi.	Store	one-off
374	E-ITS_2	NET.1.1.M3(a)	Võrgule esitatavad tehnilised nõuded on **välja töötatud** lähtuvalt võrgu turvapoliitikast (vt NET.1.1.M1 Võrgu turvapoliitika)	Store	one-off
375	E-ITS_2	NET.1.1.M5(b)	Andmesidet nende segmentide vahel reguleeritakse dünaamilise paketifiltriga (ingl dynamic packet filter). Rakenduse- ja süsteemispetsiifilised erandid, mis lubavad kliente ja servereid paigutada ühisesse võrgusegmenti, on **dokumenteeritud**.	Store	event-based
376	E-ITS_2	NET.1.1.M13(a)	On **koostatud** võrgu teostuskava, mis põhineb võrgu turvapoliitikal ja nõuete spetsifikatsioonil.	Store	one-off
377	E-ITS_2	NET.1.1.M16(a)	Arhitektuuri dokumentatsioonis **on esitatud** kõik olulised võrgu arhitektuuri komponendid, sealhulgas: • sisevõrgu arhitektuur sh virtualiseerimislahendus; • sisevõrgu liiasusega komponendid; • väliste liidestuste, sh tulemüüri ja demilitaartsooni arhitektuur; • laivõrgu ja raadiovõrgu komponendid; • turvaseadmete (tulemüürid, sissetungituvastuse ja sissetungitõrje süsteemid) asukohad ja turvafunktsioonid; • spetsiifiliste IT-süsteemide võrguühenduste nõuded; • virtualiseeritud hostide arhitektuur, sh NVO (Network Virtualization Overlay); • ühendused privaatpilvega; • ühendused pilvteenustega (vt OPS.2.2 Pilvteenuste kasutamine ja OPS.3.2 Teenuseandja infoturve); • IT-taristu halduse ja seire jaoks kasutatavate komponentide arhitektuur.	Store	one-off
378	E-ITS_2	NET.1.1.M17(a)	Võrgu arhitektuuri alusel on **koostatud** võrgu tehnilise lahenduse kava, milles on esitatud arhitektuuri elementide üksikasjad: • tsoneerimise kava; • Network Virtualization Overlay komponendid, sh virtualiseeritud võrgukomponendid; • laivõrgu ja raadiovõrgu turve; • lõppseadmete (ingl endpoint) ühendused võrguseadmetega, võrguelementide ühendused, sideprotokollid; • kõigi võrguelementide liiasusmehhanismid; • IPv4- ja IPv6-adresseerimise, kommuteerimise ja marsruutimise põhimõtted; • virtualiseeritud hostide turve; • privaatpilve komponentide turve; • IT-taristu turvalise halduse ja seire realisatsiooni määrangud.	Store	one-off
379	E-ITS_2	NET.1.1.M22(a)	Enne segmentimist on **koostatud** võrgu segmentimise eeskiri, mis arvestab kavandatavaid arhitektuuri- ja võrgulahendusi (sh ka virtualiseeritud võrke).	Store	one-off
380	E-ITS_2	NET.1.1.M25(a)	Võrgu arhitektuuri ja võrgulahenduse jaoks on **koostatud** detailne teostusplaan.	Store	one-off
381	E-ITS_2	NET.1.1.M26(a)	Võrgu haldusprotseduurid on **dokumenteeritud** võrgu käitusjuhendis	Store	one-off
382	E-ITS_2	NET.1.2.M2(a)	Võrguhalduse kavandamise käigus on **dokumenteeritud** võrguhalduse taristule ja protsessidele kehtestatud nõuded.	Store	one-off
383	E-ITS_2	NET.1.2.M11(a)	Võrguhalduseks on **koostatud** kirjalik juhend, vajadusel juhendit ajakohastatakse.	Store	event-based
384	E-ITS_2	NET.1.2.M12(a)	Võrguhalduse dokumentatsioonis **on kirjeldatud**: • hallatavad võrgukomponendid; • võrguhaldusvahendid, terminalid ja töökohad; • võrguhaldusega seotud andmebaasid ja haldusandmed; • liidesed väliste rakenduste ja teenustega.	Store	one-off
385	E-ITS_2	NET.1.2.M13(a)	On **välja töötatud** võrguhalduse kontseptsioon, mis lisaks võrguhalduse juhendis kirjeldatule (vt NET.1.2.M11 Võrguhalduse juhend) määrab: • võrguhalduse meetodid ja tehnoloogiad; • juurdepääsu ja andmeside turbe; • võrgu segmentimise; • võrguhalduse komponentide paigutuse turvatsoonides; • võrgukomponentide seire ja tegevuste logimise; • alarmeerimise korralduse; • võrguhalduse automatiseerimise; • tõrgetest ja turvaintsidentidest teatamise korralduse; • võrguhalduse avariivalmenduse.	Store	one-off
386	E-ITS_2	NET.1.2.M14(a)	Võrguhalduse kontseptsiooni ja võrguhalduse juhendi alusel on **koostatud** üksikasjalik võrguhalduse rakendusplaan.	Store	one-off
387	E-ITS_2	NET.1.2.M15(a)	Võrguhalduse taristu turvalise kasutamise kord on **välja töötatud** lähtuvalt võrgu turvapoliitikast, võrguhalduse juhendist ja võrguhalduse kontseptsioonist.	Store	one-off
388	E-ITS_2	NET.2.1.M1(a)	Raadiokohtvõrgu (ingl wireless local area network, WLAN) kasutuselevõtuks organisatsioonis on **koostatud** kava, mis määrab: • mis eesmärgil ja millistes äriprotsessides raadiokohtvõrku rakendatakse ja mis on raadiokohtvõrgu lisandväärtus; • mis asukohtades raadiovõrku rakendatakse; • milliseid funktsioone ja rakendusi raadiokohtvõrk toetab; • milliste andmete edastamiseks raadiokohtvõrku kasutada ei tohi; • milliseid turvanõudeid raadiokohtvõrgu käitamisel arvestatakse.	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
389	E-ITS_2	NET.2.1.M2(b)	Seadmete poolt toetatud raadiokohtvõrgu standarditest on valitud kasutamiseks kõige turvalisemad. Lubatud on IEEE 802.11i-2004 (krüptomehhanism WPA2) või uuem standard (WPA3). WEP ja WPA kasutamine on blokeeritud. Standardite valiku põhjused on **dokumenteeritud**.	Store	one-off
390	E-ITS_2	NET.2.1.M8(a)	Raadiokohtvõrgu intsidentide käsitlemiseks **on olemas** kord (vt DER.2.1 Turvaintsidentide käsitlus).	Store	one-off
391	E-ITS_2	NET.2.1.M10(a)	Organisatsiooni üldise turvapoliitika alusel on **dokumenteeritud**, kehtestatud ja kõigile kasutajatele teatavaks tehtud raadiokohtvõrgu turvajuhend.	Store	one-off
392	E-ITS_2	NET.2.1.M10(c)	Raadiokohtvõrgu turvajuhendi järgimist kontrollitakse regulaarselt. Tulemused **dokumenteeritakse**.	Store	event-based
393	E-ITS_2	NET.2.1.M11(a)	Raadiokohtvõrgu taristu kavandamise (vt NET.2.1.M1 Raadiokohtvõrkude kavandamine) tulemuste alusel on raadiokohtvõrgu komponentide valimiseks **koostatud** nõuete spetsifikatsioon.	Store	one-off
394	E-ITS_2	NET.2.1.M13(e)	Turvakontrollide tulemused **dokumenteeritakse**, kõrvalekallete põhjusi analüüsitakse.	Store	event-based
395	E-ITS_2	NET.2.1.M14(d)	Läbivaatuste tulemused **dokumenteeritakse**, kõrvalekallete põhjuseid analüüsitakse.	Store	event-based
396	E-ITS_2	NET.2.2.M1(a)	Organisatsiooni üldise turvapoliitika alusel on **kehtestatud** raadiokohtvõrgu (ingl wireless local area network, WLAN) kasutamise eeskiri.	Store	one-off
397	E-ITS_2	NET.2.2.M1(c)	Eeskirja järgimist kontrollitakse regulaarselt ja tulemused **dokumenteeritakse**.	Store	event-based
398	E-ITS_2	NET.3.1.M9(a)	Ruuteri ja kommutaatori olulised käidutööd (sh kõik turbe muudatustega seonduv) **lisatakse** käidudokumentatsiooni (ingl operational documentation).	Store; Update	event-based
399	E-ITS_2	NET.3.1.M10(a)	Organisatsiooni üldise turvapoliitika alusel on **kehtestatud** ruuterite (ingl router) ja kommutaatorite (ingl switch) turvajuhend, milles on esitatud seadmete turvalise käituse spetsifikatsioonid ja juhised.		one-off
400	E-ITS_2	NET.3.1.M10(c)	Lahknevused turvajuhendist ja turvajuhendi muudatused kooskõlastatakse infoturbejuhiga ning **dokumenteeritakse**.	Store; Update	event-based
401	E-ITS_2	NET.3.1.M11(a)	Ruuteri või kommutaatori hankimiseks on **kehtestatud** nõuete spetsifikatsioon.	Store	one-off
402	E-ITS_2	NET.3.1.M12(a)	Ruuterite ja kommutaatorite kasutusotstarbest tulenevalt on tähtsamate turvaseadete kontrolliks **koostatud** konfiguratsiooni kontroll-loend (ingl checklist).	Store	one-off
403	E-ITS_2	NET.3.1.M23(c)	Läbivaatuste ja läbistustestimiste tulemused **dokumenteeritakse**, tuvastatud puudustega tegeletakse esimesel võimalusel.	Store	event-based
404	E-ITS_2	NET.3.2.M1(a)	Organisatsiooni üldise turvapoliitika alusel on **kehtestatud** tulemüüride (ingl firewall) turvajuhend, milles on esitatud tulemüüride turvalise käituse nõuded.	Store	one-off
405	E-ITS_2	NET.3.2.M1(c)	Lahknevused turvajuhendist ja turvajuhendi muudatused kooskõlastatakse infoturbejuhiga ning **dokumenteeritakse**.	Store; Update	event-based
406	E-ITS_2	NET.3.2.M4(e)	Tarbetud teenused ja tarbetu lisafunktsionaalsus on tulemüüris desaktiveeritud või desinstallitud. Tulemüüri lisafunktsionaalsuse kasutuselevõtt toimub põhjendatud vajaduse alusel, vastavad otsused on **dokumenteeritud**.	Store	event-based
407	E-ITS_2	NET.3.2.M14(a)	Kõik tulemüüri turvalisust mõjutavad toimingud (sh tulemüüri reeglid, konfiguratsiooni ja süsteemiteenuste muudatused) **lisatakse** käidudokumentatsiooni (ingl operational documentation).	Store; Update	event-based
408	E-ITS_2	NET.3.2.M15(a)	Enne hankimist on tulemüüri sobivuse hindamiseks **koostatud** nõuete spetsifikatsioon.	Store	one-off
409	E-ITS_2	NET.3.2.M24(b)	Tulemüüri turbe läbivaatusi tehakse regulaarselt, läbivaatuse tulemused **dokumenteeritakse**.	Store	periodic
410	E-ITS_2	NET.3.3.M2(a)	Virtuaalse privaatvõrgu teenuseandjaga on sõlmitud teenustasemelepped (ingl service level agreement, SLA) ja need on **dokumenteeritud**.	Store	event-based
411	E-ITS_2	NET.3.3.M4(a)	Kõigi virtuaalse privaatvõrgu klientseadmete, serverite ja ühenduste jaoks on spetsifitseeritud ja **dokumenteeritud** turvaline konfiguratsioon.	Store	event-based
412	E-ITS_2	NET.3.3.M7(a)	On **koostatud** virtuaalse privaatvõrgu tehnilise teostuse kava, mis määrab: • võrgu topoloogia; • VPN pääsupunktid; • krüpteerimismeetodid ja -vahendid; • lubatavad pääsuprotokollid, • teenused ja ressursid	Store	one-off
413	E-ITS_2	NET.3.3.M8(a)	Virtuaalse privaatvõrgu kasutajate jaoks on **koostatud** virtuaalse privaatvõrgu turvalise kasutamise juhend.	Store	one-off
414	E-ITS_2	NET.3.3.M10(a)	On **dokumenteeritud** virtuaalse privaatvõrgu turvalise käituse (ingl operation) põhimõtted, milles on sätestatud virtuaalse privaatvõrgu: • kvaliteedihaldus; • järelevalve; • hooldus; • koolitus; • õiguste haldus.	Store	one-off
415	E-ITS_2	NET.3.3.M13(b)	VPN-i komponentide integratsioon tulemüüriga (ingl firewall) on **dokumenteeritud**.	Store	one-off
416	E-ITS_2	NET.3.4.M4(a)	NAC-lahenduse rakendusplaanis on **kirjeldatud** lahendusele esitatud nõuetele vastavad käitusprotseduurid ja NAC-komponentide tehnilised spetsifikatsioonid.	Store	one-off
417	E-ITS_2	NET.3.4.M11(a)	NAC-lahenduse komponentide turvaliseks konfigureerimiseks on **välja töötatud** turvalised standardkonfiguratsioonid ja protseduurijuhendid	Store	one-off
418	E-ITS_2	NET.3.4.M18(a)	NAC-lahendus koos kõigi lahendusse kuuluvate komponentidega on asjakohaselt **dokumenteeritud**.	Store	one-off
419	E-ITS_2	NET.4.1.M1(a)	Enne telefonikeskjaama hankimist või laiendamist on **tehtud** sidesüsteemi nõuete analüüs.	Store	one-off
420	E-ITS_2	NET.4.1.M6(a)	Organisatsiooni turvapoliitikate alusel on **kehtestatud** telefonikeskjaama turvajuhend.	Store	one-off
421	E-ITS_2	NET.4.1.M10(a)	Telefonikeskjaama konfiguratsioon ja telefoninumbrite loend on **dokumenteeritud** ja ajakohastatud.	Store	event-based
422	E-ITS_2	NET.4.1.M12(a)	On **koostatud** sidesüsteemide andmevarunduse kontseptsioon, mis on osa serverite ja võrgukomponentide üldisest andmevarunduse kontseptsioonist.	Store	one-off
423	E-ITS_2	NET.4.2.M1(a)	Enne IP-telefonide kasutuselevõttu on **koostatud** VoIP-põhise sidesüsteemi kasutuselevõtu kava.	Store	one-off
424	E-ITS_2	NET.4.2.M5(b)	Kõik installimis- ja konfigureerimisetapid on **dokumenteeritud** selliselt, et pädev kolmas isik on võimeline vahetarkvara seadistama, tuginedes ainult dokumentatsioonile.	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
425	E-ITS_2	NET.4.2.M5(c)	Konfigureerimise automatiseerimise makrod on põhjalikult testitud ja **dokumenteeritud**.	Store	event-based
426	E-ITS_2	NET.4.2.M7(a)	Organisatsiooni üldise turvapoliitika alusel on **kehtestatud** VoIP-põhise sidesüsteemi turvajuhend, mis esitab VoIP-põhise sidesüsteemi komponentide käitus- ja kasutusnõuded.	Store	one-off
427	E-ITS_2	NET.4.2.M9(a)	VoIP-põhise sidesüsteemi komponentide valimiseks on **koostatud** nõuete spetsifikatsioon.	Store	one-off
428	E-ITS_2	NET.4.2.M15(e)	Krüptomehhanismide ja -parameetrite ning räsialgoritmi valik ja põhjendus on **dokumenteeritud**.	Store	event-based
429	E-ITS_2	SYS.1.1.M6(d)	Serveri tarkvara, teenuste ja kontode konfiguratsioon on **dokumenteeritud**.	Store	one-off
430	E-ITS_2	SYS.1.1.M10(a)	On kehtestatud ja **dokumenteeritud**, milliseid sündmusi serveris logitakse ning kes ja millistel tingimustel võib logiandmeid vaadata.	Store	one-off
431	E-ITS_2	SYS.1.1.M11(a)	Organisatsiooni üldisest turvapoliitikast lähtuvalt on **dokumenteeritud** ja kehtestatud serveri turvajuhend. Turvajuhend arvestab serverite erinevat kaitsetarvet.	Store	one-off
432	E-ITS_2	SYS.1.1.M11(d)	Juhendis esitatu täitmist kontrollitakse regulaarselt, kontrollide tulemused **dokumenteeritakse**.	Store	event-based
433	E-ITS_2	SYS.1.1.M12(b)	Serveri kasutuselevõtu kavandamisel tehtud otsused on **dokumenteeritud**.	Store	event-based
434	E-ITS_2	SYS.1.1.M16(d)	Serveri aluskonfiguratsioon on **dokumenteeritud**, isegi juhul kui kasutatakse tootjapoolseid vaikeseadistusi.	Store	one-off
435	E-ITS_2	SYS.1.1.M21(a)	Serveri käitusega seotud toimingud, sooritajad ja toimingu tulemid on arusaadavalt **dokumenteeritud** serveri käidudokumentatsioonis (ingl operational documentation).	Store	event-based
436	E-ITS_2	SYS.1.1.M22(c)	Talitluspidevust mõjutavate serveriteenuste taasteks ja taaskäivituseks on **dokumenteeritud** ja kehtestatud taastekava (ingl disaster recovery plan)	Store	one-off
437	E-ITS_2	SYS.1.1.M24(e)	Kontrolli tulemused **dokumenteeritakse** ja lahknevusi käsitletakse esimesel võimalusel.	Store	event-based
438	E-ITS_2	SYS.1.1.M25(b)	Serveri kõrvaldamiseks on **koostatud** toimingute kontroll-loend, mis käsitleb vähemalt andmete varundamist, teenuste üleviimist ja andmete turvalise kustutamisega seotud aspekte.	Store	event-based
439	E-ITS_2	SYS.1.1.M39(b)	Serveri turvaseaded vastavad kehtestatud turvapoliitikatele ja -juhenditele. Erandid **dokumenteeritakse** koos põhjendusega.	Store	event-based; one-off
440	E-ITS_2	SYS.1.1.M27(d)	Anomaaliatest teavitamiseks ja anomaaliate käsitlemiseks on kehtestatud kord.	Store	one-off
441	E-ITS_2	SYS.1.1.M33(a)	Serveri tööks vajalike juursertifikaatide loend on **dokumenteeritud**.	Store	one-off
442	E-ITS_2	SYS.1.2.3.M1(a)	Kasutusele võetav Windows Serveri väljalase on valitud põhjendatud ja **dokumenteeritud** valikukriteeriumite alusel.	Store	event-based
443	E-ITS_2	SYS.1.2.3.M2(a)	Kui olemasolevast funktsionaalsusest piisab, installitakse minimaalvariant Server Core. Muude funktsioonide lisamiseks on **olemas** kirjalik põhjendus.	Store	event-based
444	E-ITS_2	SYS.1.5.M10(a)	On kehtestatud ja **dokumenteeritud** protseduurid virtuaalserverite ja virtualiseeritud IT-süsteemide kasutuselevõtuks, arvestuseks, käitamiseks ja kasutuselt kõrvaldamiseks.	Store	one-off
445	E-ITS_2	SYS.1.5.M12(a)	On **kehtestatud** virtualiseerimisserveri halduseks vajalikud õigused ja rollid (vt SYS.1.5.M8 Virtualiseerimissüsteemi kavandamine).	Store	one-off
446	E-ITS_2	SYS.1.5.M19(c)	Läbivaatuste tulemused **dokumenteeritakse** ja tuvastatud lahknevused kõrvaldatakse esimesel võimalusel.	Store	event-based
447	E-ITS_2	SYS.1.6.M1(d)	Konteinerduse eesmärgid, riski- ja kuluhinnangud on **dokumenteeritud**.	Store	one-off
448	E-ITS_2	SYS.1.6.M4(a)	Konteineritõmmiste loomise ja rakendamise protsess on piisava detailsusega kavandatud ja **dokumenteeritud**.	Store	one-off
449	E-ITS_2	SYS.1.6.M9(c)	Rakenduste konteineris käitamise sobivuse kontrollid (vt SYS.1.6.M3 Konteinerdatud IT-süsteemide turvaline käitamine) on **dokumenteeritud**.	Store	event-based
450	E-ITS_2	SYS.1.6.M10(b)	On **loodud** ja rakendatud eeskiri, mis määrab konteinerite käitamise reeglid.	Store	one-off
451	E-ITS_2	SYS.1.6.M20(b)	Kõik konfiguratsioonimuudatused on selgesõnaliselt **dokumenteeritud**.	Store	event-based
452	E-ITS_2	SYS.1.6.M21(a)	On **koostatud** täpsed eeskirjad konteinerite pääsuõiguste halduseks.	Store	one-off
453	E-ITS_2	SYS.1.8.M6(a)	Organisatsiooni üldise turvapoliitika alusel on **koostatud** salvestilahenduste turvajuhend, mis sisaldab nõudeid salvestilahenduse turvaliseks kavandamiseks, rakendamiseks, halduseks, käituseks ja kõrvaldamiseks.	Store	one-off
454	E-ITS_2	SYS.1.8.M6(d)	Turvajuhendi rakendamist kontrollitakse regulaarselt. Kontrolli tulemused **dokumenteeritakse**.	Store	event-based
455	E-ITS_2	SYS.1.8.M7(b)	Nõuete spetsifikatsiooni alusel on **koostatud** salvestilahenduse rakendamise kava, mis määratleb: • sobiva riistvaraspetsifikatsiooni; • valmistaja ja tarnija valimise kriteeriumid; • hangitava lahenduse arhitektuuri (tsentraliseeritud või hajutatud); • võrguühenduste kava; • vajaliku infrastruktuuri; • integratsiooni olemasolevate protsessidega.	Store	one-off
456	E-ITS_2	SYS.1.8.M8(b)	Salvestilahenduse valikukriteeriumid on üheselt arusaadavalt **dokumenteeritud**.	Store	one-off
457	E-ITS_2	SYS.1.8.M8(d)	Salvestilahenduse valimise otsus koos valikukriteeriumitele vastavuse põhjendusega on **dokumenteeritud**.	Store	one-off
458	E-ITS_2	SYS.1.8.M10(a)	On **koostatud** salvestilahenduse käitamise juhend, mis esitab käitamise protsessid, nõuded ja konfiguratsiooni.	Store	one-off
460	E-ITS_2	SYS.1.8.M14(a)	Salvestusvõrgu (ingl storage area network, SAN) ressursside jaotus serveritele on **dokumenteeritud**.	Store	event-based
461	E-ITS_2	SYS.1.8.M14(d)	Kehtiv tsoonimiskonfiguratsioon on **dokumenteeritud**. Dokumentatsioon on kättesaadav ka avarii korral.	Store	one-off
462	E-ITS_2	SYS.1.8.M15(a)	Organisatsiooni nõuded salvestilahenduse simultaanteenindusvõimele (ingl multi-tenancy) on määratud ja **dokumenteeritud**	Store	one-off
463	E-ITS_2	SYS.1.8.M15(b)	Salvestilahendus vastab **dokumenteeritud** lahususenõuetele.	Store	one-off
464	E-ITS_2	SYS.1.8.M17(a)	Salvestisüsteemide konfiguratsioon (sh spetsiifilised süsteemikonfiguratsioonid) on **dokumenteeritud**.	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
465	E-ITS_2	SYS.1.8.M18(a)	On **kehtestatud** kord salvestisüsteemide regulaarseks läbivaatuseks ja seda järgitakse.	Store	one-off
466	E-ITS_2	SYS.1.8.M20(a)	On **koostatud** salvestilahenduse avariikava, mis annab täpsed juhised avariiolukorras tegutsemiseks.	Store	one-off
467	E-ITS_2	SYS.1.9.M1(a)	Organisatsioon on **dokumenteerinud** ja kehtestanud terminaliserveri turvanõuded. Turvanõuded käsitlevad vähemalt järgnevaid teemasid: • terminaliserveritesse installitav tarkvara; • rakendused, mis on lubatud läbi terminaliserveri kasutada; • turvanõuded klientidele või klienditarkvara kasutavatele klientarvutitele, sh füüsilise turbe nõuded; • võrguturve, sh lubatavad andmesideprotokollid ning nõuded kliendi võrgule; • klientide ja terminaliserverite vahelised krüpteerimismehhanismid ja autentimismeetodid; • lisaks tavapäraste sisend- ja väljundseadmetele kliendiga täiendavalt ühendatavad välisseadmed.	Store	one-off
468	E-ITS_2	SYS.1.9.M2(a)	On **dokumenteeritud** terminaliserveris käitatavatele rakendustele esitatavad funktsionaalsed nõuded.	Store	event-based
469	E-ITS_2	SYS.1.9.M4(a)	Terminaliserveritele on kehtestatud ja **dokumenteeritud** rakenduste turva- ja funktsionaalsusnõuetest lähtuvad tüüpkonfiguratsioonid.	Store	one-off
470	E-ITS_2	SYS.2.1.M6(b)	Erandjuhud, kui kahjurvaratõrje rakendust klientarvutisse ei paigaldata, on põhjendatud ja **dokumenteeritud**.	Store	event-based
471	E-ITS_2	SYS.2.1.M9(a)	Organisatsiooni üldise turvapoliitika alusel on **kehtestatud** klientarvutite kaitsetarbele vastav klientarvuti turvalise kasutamise juhend.	Store	one-off
472	E-ITS_2	SYS.2.1.M9(e)	Juhendi järgimist kontrollitakse regulaarselt. Kontrolli tulemused **dokumenteeritakse**.	Store	event-based
473	E-ITS_2	SYS.2.1.M42(b)	Klientarvutites lubatavad pilve- ja võrgufunktsioonid on **dokumenteeritud**.	Store	one-off
474	E-ITS_2	SYS.2.1.M10(a)	Klientarvutite profileerimiseks, turvaliseks rakendamiseks ja käituseks on **koostatud** klientarvutite kasutuselevõtu kava.	Store	one-off
475	E-ITS_2	SYS.2.1.M10(d)	Kavandamisfaasis tehtud otsused on **dokumenteeritud**.	Store	event-based
476	E-ITS_2	SYS.2.1.M15(c)	Klientarvutite seadistamiseks on koostatud ja **dokumenteeritud** turvaline aluskonfiguratsioon. Aluskonfiguratsioon sisaldab vähemalt järgmisi aspekte: • haldusõigustega kontod; • süsteemikataloogid- ja failid; • kasutajakontod ja -kataloogid; • võrkupääs; • lokaalsed turvafunktsioonid (nt paketifilter); • seirefunktsioonid (sh kasutusinfo tootjale edastamise (nn Phone Home) funktsioonid).	Store	one-off
477	E-ITS_2	SYS.2.1.M16(d)	Tarbetute komponentide desaktiveerimise otsused on **dokumenteeritud**.	Store	event-based
478	E-ITS_2	SYS.2.1.M20(a)	Klientarvuti tavapäraste haldustööde jaoks on **koostatud** haldusjuhis, mis hõlmab vähemalt järgmist: • kasutajate loomine ja desaktiveerimine; • rakenduste installimine ja desinstallimine; • turvauuendite ja turbepaikade paigaldamine; • uute rakenduste paigaldamine; • regulaarne tervikluse kontroll.	Store	one-off
479	E-ITS_2	SYS.2.1.M21(a)	Klientarvuti mikrofoni ja kaamera kasutamiseks on **kehtestatud** kord.	Store	one-off
480	E-ITS_2	SYS.2.1.M27(c)	Klientarvuti kõrvaldamiseks koostatakse alati kontroll-loend, mis määrab: • millised andmed tuleb enne arvuti kõrvaldamist varundada või arhiveerida ja kuidas; • millised kõrvaldatava arvutiga seotud õigused, viited ja kirjed tuleb kõrvaldada; • millised jääkandmed ja varundatud andmed tuleb kustutada ja kuidas.	Store	event-based
481	E-ITS_2	SYS.2.1.M30(d)	Testimiseks on koostatud tüüpstsenaariumid, testitulemused **dokumenteeritakse**.	Store	event-based
482	E-ITS_2	SYS.2.1.M28(b)	Krüpteerimise konfiguratsioon ning krüpteerimise ja dekrüpteerimise protsessid on **dokumenteeritud**.	Store	one-off
483	E-ITS_2	SYS.2.1.M35(a)	Klientarvuti ettevalmistamisel **dokumenteeritakse** klientarvuti tööks vajalikud juursertifikaadid.	Store	event-based
484	E-ITS_2	SYS.2.1.M38(d)	On **koostatud** klientarvuti avariikava, milles on määratud järgnev: • varuosade olemasolu või nende saamine hooldelepingute raames; • taastekäivitustrigerid ja taastamise prioriteedid; • paroolide ja krüptovõtmete asukohad; • taasteplaan (süsteemi järkjärgulise taastamise protseduuri); • süsteemi konfiguratsiooni dokumentatsioon; • taasteks vajalik lisatarkvara ja -riistvara.	Store	one-off
485	E-ITS_2	SYS.2.1.M40(a)	Klientarvuti hooldustööd on selgelt **dokumenteeritud**. Dokumentatsioon sisaldab, kes ja millal töid teostas ning mis oli hooldustöö sisu.	Store	event-based
486	E-ITS_2	SYS.2.2.3.M9(c)	Kasutatavad krüptomehhanismid vastavad kaitsetarbele ning on **dokumenteeritud**.	Store	one-off
487	E-ITS_2	SYS.2.2.3.M20(b)	UAC konfiguratsioon on **dokumenteeritud**.	Store	one-off
488	E-ITS_2	SYS.2.3.M12(b)	Spetsiaalseadmetele kehtivad turvanõuded on **dokumenteeritud**	Store	event-based
489	E-ITS_2	SYS.2.4.M1(a)	macOS-i klientide kasutuselevõtuks on **koostatud** kava	Store	one-off
490	E-ITS_2	SYS.3.1.M1(a)	Organisatsioonis on **kehtestatud** sülearvutite mobiilse kasutamise kord, mis määrab: • milliseid sülearvuteid on lubatud väljaspool organisatsiooni kasutada; • kes tohib neid kaasas kanda; • milliseid turvameetmeid tuleb rakendada; • milline on kasutaja vastutus.	Store	one-off
491	E-ITS_2	SYS.3.1.M12(a)	Organisatsioonis on **kehtestatud** kord sülearvuti kaotamisest, vargusest või rikkest teavitamiseks.	Store	one-off
492	E-ITS_2	SYS.3.1.M6(a)	Organisatsioonis on koostatud ja **kehtestatud** sülearvuti kasutamise eeskiri.	Store	one-off
493	E-ITS_2	SYS.3.1.M15(a)	Enne sülearvutite hankimist on sülearvutite kasutusotstarbe põhjal **koostatud** nõuded riist- ja tarkvarakomponentidele.	Store	event-based
494	E-ITS_2	SYS.3.1.M16(a)	On **kehtestatud** keskse sülearvutite halduse protseduur (vt SYS.3.2.2 Mobiilseadmete haldus (MDM))	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
495	E-ITS_2	SYS.3.2.1.M1(a)	On **kehtestatud** nutitelefonide ja tahvelarvutite kasutamise eeskiri, mis sisaldab vähemalt järgmist: • nõutavad autentimis- ja pääsumehhanismid ja nende rakendamine; • nõuded nutitelefonide ja tahvelarvutite turvaliseks ja heaperemehelikuks kasutamiseks; • nõuded nutitelefonide ja tahvelarvutite varguse vältimiseks; • lubatavad teenused; • tingimused organisatsiooni ressurssidele juurdepääsu saamiseks; • mobiilseadmete soetamise ja kuluarvestuse kord; • isiklike mobiilseadmete tööalase kasutamise kord; • juhised mobiilseadme kaotuse, varguse või rikke puhul tegutsemiseks.	Store	one-off
496	E-ITS_2	SYS.3.2.1.M2(a)	On **kehtestatud** nutitelefonide ja tahvelarvutite turvalise pilvekasutuse kord, millega määratakse, millised pilvteenused on kasutamiseks lubatud ja kuidas töötajate pilvkasutust kontrollitakse.	Store	one-off
497	E-ITS_2	SYS.3.2.1.M3(b)	On koostatud ja **dokumenteeritud** turvamehhanisme toetav nutitelefonide ja tahvelarvutite aluskonfiguratsioon.	Store	one-off
498	E-ITS_2	SYS.3.2.1.M10(a)	On **koostatud** nutitelefonide ja tahvelarvutite keskse halduse juhend.	Store	one-off
499	E-ITS_2	SYS.3.2.1.M31(a)	Organisatsioonis on **kehtestatud** kord, mis reguleerib nutitelefonidest ja tahvelarvutitest tehtavaid mobiilmakseid ja nende hüvitamist.	Store	one-off
500	E-ITS_2	SYS.3.2.2.M1(c)	Mobiilseadmete halduse põhimõtted on **dokumenteeritud** ning kooskõlastatud infoturbejuhiga	Store	one-off
501	E-ITS_2	SYS.3.2.2.M5(a)	Mobiilseadmete tarbeks on koostatud ja **dokumenteeritud** sobivad aluskonfiguratsioonid.	Store	one-off
502	E-ITS_2	SYS.3.2.3.M1(a)	On välja töötatud ja **dokumenteeritud** iOS-põhiste seadmete rakendamise põhimõtted, milles on käsitletud: • iOS-põhiste seadmete valimise kriteeriumid; • iOS-põhiste seadmete haldus ja konfigureerimine; • valideerimata rakenduste kasutamine; • varundusstrateegia.	Store	one-off
503	E-ITS_2	SYS.3.2.3.M10(b)	Kasutajatele on **koostatud** biomeetrilise autentimise juhend.	Store	one-off
504	E-ITS_2	SYS.3.3.M7(a)	Enne mobiiltelefonide hankimist on **koostatud** nõuete spetsifikatsioon	Store	event-based
505	E-ITS_2	SYS.3.3.M11(a)	Olulised mobiiltelefonide pääsu- ja konfiguratsiooniandmed on **dokumenteeritud**.	Store	periodic
506	E-ITS_2	SYS.3.3.M12(b)	Mobiiltelefonide ja tarvikute väljastamine ja tagastamine **dokumenteeritakse**	Store	event-based
507	E-ITS_2	SYS.4.1.M1(a)	Organisatsioon on koostanud ja dokumenteerinud printerite ja kontorikombainide rakendamise kava, mis määrab: • millised on printerite ja kontorikombainide vajalikud funktsioonid ja tootlus; • kas printerid ja kontorikombainid ostetakse või renditakse; • kas kasutatakse lokaalseid või võrgustatud seadmeid; • kellel on printerite ja kontorikombainide kasutus- ja haldusõigused; • milliste ohtude eest tuleb seadmeid kaitsta; • millised on andmeedastuse ja seadme füüsilise turbe nõuded; • mis on nõutavad andmeedastusprotokollid ja failivormingud; • kuidas on takistatud juurdepääs võõrastele dokumentidele; • kuidas korraldatakse printerite ja kontorikombainide hooldust ja kulumaterjalidega varustamist; • kuidas tagatakse printerite ja kontorikombainide käideldavus; • kuidas korraldatakse kasutajate ja haldajate koolitus.	Store	one-off
508	E-ITS_2	SYS.4.1.M2(b)	Printereid ja kontorikombaine haldavad ainult haldusõigusega isikud. Teenuseandjaga (nt hoolduseks ja remondiks) on **sõlmitud** kirjalikud konfidentsiaalsuskokkulepped.	Store	one-off
509	E-ITS_2	SYS.4.1.M5(a)	Infoturbejuht on printerite ja kontorikombainide kasutajatele **koostanud** eeskirja printerite ja kontorikombainide turvaliseks käsitsemiseks.	Store	one-off
510	E-ITS_2	SYS.4.1.M22(a)	Tarbetute tundlikku teavet sisaldavate dokumentide kõrvaldamiseks on **kehtestatud** kord.	Store	one-off
511	E-ITS_2	SYS.4.1.M4(a)	Organisatsioonis on koostatud ja **dokumenteeritud** printerite ja kontorikombainide turvaeeskiri, mis sätestab seadmetes andmete töötlemise turvanõuded ja tingimused.	Store	one-off
512	E-ITS_2	SYS.4.3.M1(b)	Kõik sardsüsteemid ja sardsüsteemide liidesed on **dokumenteeritud**	Store	one-off
513	E-ITS_2	SYS.4.3.M1(c)	On **kehtestatud** sardsüsteemide tervikluse ja töövõimelisuse testimise kord.	Store	one-off
514	E-ITS_2	SYS.4.3.M1(d)	Sardsüsteemid on turvaliselt eelseadistatud. Kasutatavad konfiguratsioonid on **dokumenteeritud**.	Store	one-off
515	E-ITS_2	SYS.4.3.M4(a)	Sardsüsteemi hankimiseks on **koostatud** nõuete spetsifikatsioon mille alusel süsteeme või komponente hinnatakse.	Store	event-based
516	E-ITS_2	SYS.4.3.M11(c)	Andmete kustutamine ja riistvara hävitamine **dokumenteeritakse**.	Store	event-based
517	E-ITS_2	SYS.4.3.M16(d)	Muukimisintsidendile reageerimiseks on **koostatud** juhend.	Store	one-off
518	E-ITS_2	SYS.4.4.M1(a)	Esemevõrgu seadmete jaoks on **koostatud** minimaalselt vajalikud turvanõuded, millele kõik organisatsioonis kasutatavad IoT seadmed peavad vastama.	Store	one-off
519	E-ITS_2	SYS.4.4.M6(a)	Poliitika nõuete järgmist kontrollitakse regulaarselt. Kontrolli tulemused **dokumenteeritakse**.	Store	event-based
520	E-ITS_2	SYS.4.4.M7(a)	Esemevõrgu seadmete rakendamise kava **sisaldab** vähemalt järgmist: • esemevõrgu otstarve ja teenused; • kasutuskohad ja kasutusviis; • autentimise vajadus ja tüüp; • seadmete haldus; • võrguühendused ja võrguteenused; • logimine; • turvamehhanismid.	Store	one-off
521	E-ITS_2	SYS.4.4.M7(b)	Kõik kavandamise etapis tehtud otsused **dokumenteeritakse**.	Store	event-based
522	E-ITS_2	SYS.4.4.M10(b)	Kõik installimis- ja konfigureerimisetapid on **dokumenteeritud** nii, et pädev kolmas isik suudaks protseduuri dokumentatsiooni põhjal läbi viia.	Store; Update	event-based
523	E-ITS_2	SYS.4.4.M20(c)	IoT-seadmete kasutusest kõrvaldamiseks **luuakse** kontrollnimekiri, mis sisaldab vähemalt vajalikke andmete varundamise ja turvalise kustutamise aspekte; muuhulgas arvestatakse andmeid, mis olid salvestatud pilve või irdandmekandjale.	Store	event-based

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
524	E-ITS_2	SYS.4.5.M4(a)	Organisatsioonis on **koostatud** irdandmekandjate kasutamise eeskiri.	Store	one-off
525	E-ITS_2	SYS.4.5.M5(a)	Irdandmekandjate väljaviimise kohta on **kehtestatud** kord, mis määrab: • kas, millal ja milliseid irdandmekandjaid tohib organisatsiooni territooriumilt välja viia; • kes ja kuidas tohivad irdandmekandjaid välja viia; • milliseid turvameetmeid (eelkõige andmete krüpteerimist) tuleb seejuures rakendada.	Store	one-off
526	E-ITS_2	SYS.4.5.M6(a)	Irdandmekandjate halduseks on **kehtestatud** ühtsed reeglid.	Store	one-off
527	E-ITS_2	SYS.4.5.M7(b)	Andmete turvaliseks kustutamiseks on **koostatud** juhised. Töötajatel on juurdepääs turvalist kustutamist võimaldavatele vahenditele.	Store	one-off
528	E-ITS_2	SYS.EE.1.M21(a)	On **kehtestatud** turvaserveri teenuse standardtingimused ...	Store	one-off
529	E-ITS_2	SYS.EE.1.M21(b)	Teenussoovid ning tehtud muutused teenuse tarbijat puudutavates seadistustes dokumenteeritakse.	Store	event-based
530	E-ITS_2	SYS.EE.1.M22(c)	On **dokumenteeritud** turvaserveri taasteplaan. Taasteplaani toimimist testitakse regulaarselt.	Store	one-off
531	E-ITS_2	APP.1.1.M6(b)	Kontoritarkvara võetakse esmalt pilootkasutusse, et veenduda toote toimimises käidukeskkonnas ning tegelike andmetega. Pilootkasutuse tulemused **dokumenteeritakse**.	Store	event-based
532	E-ITS_2	APP.1.1.M10(a)	Eksisteerib **kirjalik** otsus, kas kasutajate tehtud kontoritarkvara lisaarendused (nt makrode ja lingitud arvutustabelite abil) on organisatsioonis lubatud.	Store	one-off
533	E-ITS_2	APP.1.1.M10(c)	Organisatsioonis on **kehtestatud** kontoritarkvara lisaarenduste tegemise kord, mis määratleb dokumenteerimise ja testimise nõuded, vastutavate töötajate kompetentsid ja tulemi kasutuselevõtu protseduurid.	Store	one-off
534	E-ITS_2	APP.1.1.M10(d)	Kasutaja loodud lisaarendused **dokumenteeritakse** ja dokumentatsioon tehakse töötajaile kättesaadavaks.	Store	event-based
535	E-ITS_2	APP.2.1.M1(a)	On **koostatud** üldisele infoturvapoliitikale vastav kataloogiteenuse turvaeeskiri.	Store	one-off
536	E-ITS_2	APP.2.1.M2(b)	Kataloogiteenuse rakenduskavas on dokumenteeritud: • kataloogiteenuse struktuur; • ettenähtud kasutusviisidega sobiv objektiklasside ja atribuuditüüpide mudel; • vajadustel põhinev pääsuõiguste haldusmudel; • isikuandmeid sisaldava kataloogiteenuse kavandamisel on kaasatud andmekaitsespetsialist.	Store	one-off
537	E-ITS_2	APP.2.1.M3(a)	Kataloogiteenuse ja selle andmete haldustegevusi hoitakse omavahel lahus. Haldusülesanded **dokumenteeritakse**, ülesandeid täitvad isikud ei talitle konfliktsetes rollides.	Store	event-based
538	E-ITS_2	APP.2.1.M6(a)	Kataloogiteenuse halduse ja käituse protsessid on **dokumenteeritud**.	Store	one-off
539	E-ITS_2	APP.2.1.M15(a)	Kataloogiteenuse migreerimiseks **koostatakse** eelnevalt migratsioonikava. Kataloogiteenuse skeemi kavandatud muudatused **dokumenteeritakse**.	Store	event-based
540	E-ITS_2	APP.2.1.M18(a)	Kataloogiteenuse dubleerimise kavandamisel määratakse dubleerimise eesmärgid ning **koostatakse** rakendusstsenaariumit ja võrgutopoloogiat kirjeldav tegevusplaan.	Store	one-off
541	E-ITS_2	APP.2.1.M16(a)	Avariivalmenduse raames on kehtestatud ja **dokumenteeritud** organisatsiooni vajadustele vastav kataloogiteenuse avariikava.	Store	one-off
542	E-ITS_2	APP.2.2.M1(b)	On **kehtestatud** vajaduse- ja rollipõhine AD õiguste kontseptsioon ja õiguste delegeerimise kord.	Store	one-off
543	E-ITS_2	APP.2.2.M1(c)	AD DS kavandamisel on dokumenteeritud: • AD struktuur ning AD domeenide jaotus AD puudesse (ingl AD tree) ja AD metsadesse (ingl AD forest); • AD liidendusteenuse (ingl Active Directory Federation Service- ADFS) kasutamine ja usaldusseosed; • rühmapoliitikate rakendamise kontseptsioon; • kasutajate ja arvutite kuuluvus domeenidesse.	Store	one-off
544	E-ITS_2	APP.2.2.M3(a)	Konfiguratsioonisätete (sh turvasätete) kogumiku rakendamine objektirühmadele toimub **dokumenteeritud** rühmapoliitikate alusel.	Store	one-off
545	E-ITS_2	APP.2.2.M5(j)	Domeenikontrolleri jaoks on **koostatud** taasteplaan. Ühe taastevõimalusena on võimalik domeenikontroller buutida AD taasterežiimis (ingl Directory Services Restore Mode, DSRM).	Store	one-off
546	E-ITS_2	APP.2.3.M3(e)	Pärast iga muudatust Slapd-serveri konfiguratsioon kontrollitakse ja **dokumenteeritakse**.	Store	event-based
547	E-ITS_2	APP.3.1.M1(b)	Autentimisviisid on turvalised ja nende valik on **dokumenteeritud**.	Store	event-based
548	E-ITS_2	APP.3.1.M8(e)	Veebirakenduse tarkvaraarhitektuur koos kõikide komponentide ja sõltuvustega on **dokumenteeritud**. Dokumentatsioonis on välja toodud ka rakendusevälised, kuid rakenduse tööks vajatavad komponendid.	Store	one-off
549	E-ITS_2	APP.3.1.M9(a)	Veebirakenduse komponentide hankimiseks on **kehtestatud** nõuded tootele ja kokku lepitud hindamisskaala.	Store	one-off
550	E-ITS_2	APP.3.1.M22(b)	Läbivaatuste ja läbistustestimiste tulemused **dokumenteeritakse**. Neid käsitletakse konfidentsiaalsetena ja säilitatakse turvaliselt.	Store	event-based
551	E-ITS_2	APP.3.2.M1(a)	Pärast veebiserveri installimist on loodud ja **dokumenteeritud** turvaline aluskonfiguratsioon.	Store	event-based
552	E-ITS_2	APP.3.2.M8(a)	Veebiserveri rakendamiseks on **koostatud** kava, kus on dokumenteeritud veebiserveri kasutamise eesmärk, esitatavad andmed, kasutajate sihtrühm ja olemasolevasse IT-taristusse integreerimise protsess.	Store	one-off
553	E-ITS_2	APP.3.2.M9(a)	On kehtestatud ja **dokumenteeritud** veebiserveri turvapoliitika, mis määrab veebiserveri infoturbe meetmed ja vastutajad.	Store	one-off
554	E-ITS_2	APP.3.2.M16(b)	Testimise ja läbivaatuse tulemused **dokumenteeritakse**, neid hoitakse konfidentsiaalsena.	Store	event-based
555	E-ITS_2	APP.3.3.M2(a)	Organisatsioon on analüüsinud, kas ja millist RAID-süsteemi on failiserveris otstarbekas kasutada. RAIDi mittekasutamine on koos põhjendusega **dokumenteeritud**.	Store	event-based
556	E-ITS_2	APP.3.3.M15(a)	Failiserveri kasutusele võtmiseks on **tehtud** eelanalüüs, mis määratleb serveri otstarbele vajaliku funktsionaalsuse ja piirangud	Store	one-off
557	E-ITS_2	APP.3.3.M6(a)	Failiserveri hankimiseks on **koostatud** failiserveri nõuete spetsifikatsioon, mille põhjal tooteid võrreldakse.	Store	one-off
558	E-ITS_2	APP.3.4.M1(a)	Enne Samba serveri kasutuselevõttu on otsustatud ja **dokumenteeritud**: • milliseid ülesandeid Samba server tulevikus täidab;	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
			• millisel tööviisil Samba töötab; • kuidas teostatakse autentimine; • milline peab olema Samba töökeskkond; • milliseid Samba ja muid komponente on selleks vaja.		
559	E-ITS_2	APP.3.6.M1(a)	DNSi rakendamise kavandamisel on otsustatud ja **dokumenteeritud**: • DNS teenuse ülesehitus; • kaitstav domeeniinfo; • DNS-serverite integreerimisviis; • DNS-teenusega seotud kasutajarollid.	Store	one-off
560	E-ITS_2	APP.3.6.M9(a)	DNS-serveri jaoks on **koostatud** avariikava, mis on kooskõlas organisatsiooni olemasolevate avariikavade ja jätkusuutlikkusplaaniga (vt DER.4 Avariihaldus).	Store	one-off
561	E-ITS_2	APP.4.3.M1(a)	Organisatsiooni üldise infoturvapoliitika põhjal on **koostatud** andmebaasisüsteemi turvaeeskiri, mis esitab andmebaaside turvalise kasutuse nõuded.	Store	one-off
562	E-ITS_2	APP.4.3.M1(c)	Eeskirja nõuetest kõrvale kaldumine **dokumenteeritakse** ja sellest teavitatakse infoturbejuhti.	Store; Provide	event-based
563	E-ITS_2	APP.4.3.M1(d)	Andmebaasisüsteemi turvaeeskirja järgimist kontrollitakse regulaarselt, tulemused **dokumenteeritakse**.	Store	event-based
564	E-ITS_2	APP.4.3.M3(a)	Andmebaasihalduse süsteemi tugevdamise meetmetest on **koostatud** kontroll-loend.	Store	one-off
565	E-ITS_2	APP.4.3.M4(a)	Andmebaaside loomiseks ja kasutuselevõtuks on **kehtestatud** protseduur.	Store	one-off
566	E-ITS_2	APP.4.3.M4(b)	Teave kasutuselevõetava andmebaasi kohta **dokumenteeritakse** kokkulepitud kujul.	Store	event-based
567	E-ITS_2	APP.4.3.M12(a)	Andmebaasihalduse süsteemide jaoks on **koostatud** ühtne tüüpkonfiguratsioon.	Store	one-off
568	E-ITS_2	APP.4.3.M13(b)	Andmebaasilingid on **dokumenteeritud** ja neid kontrollitakse regulaarselt.	Store	periodic
569	E-ITS_2	APP.4.3.M17(a)	On **koostatud** protseduurid andmete laadimiseks ja migreerimiseks andmebaasi.	Store	one-off
570	E-ITS_2	APP.4.3.M19(b)	Enne andmebaasiskripti rakendamist viiakse läbi funktsionaaltestid, tulemused **dokumenteeritakse**.	Store	event-based
571	E-ITS_2	APP.4.3.M20(c)	Läbivaatuste tulemused on **dokumenteeritud**.	Store	event-based
572	E-ITS_2	APP.4.3.M22(a)	Andmebaasisüsteemi intsidendi puhul käitumiseks ning andmebaaside tavapärase seisundi taastamiseks on **koostatud** avariikava.	Store	one-off
573	E-ITS_2	APP.4.3.M23(a)	Andmebaasisüsteemi andmete arhiveerimiseks on **koostatud** andmebaasisüsteemi arhiveerimiskava.	Store	one-off
574	E-ITS_2	APP.4.3.M23(c)	Arhiveeritud andmete taastamist harjutatakse regulaarselt, tulemused **dokumenteeritakse**.	Store	event-based
575	E-ITS_2	APP.4.4.M1(c)	Kavandamise käigus on **koostatud** võrgu, CPU ja püsimälu eraldamise reeglid.	Store	one-off
576	E-ITS_2	APP.5.2.M1(a)	Microsoft Exchange'i ja Outlooki rakendamise kava **koostamisel** on arvestatud vähemalt järgmist: • meilitaristu struktuur; • Microsoft Exchange'iga ühenduvad klient- ja serversüsteemid; • funktsioonilaienduste kasutamine; • kasutatavad protokollid.	Store	one-off
577	E-ITS_2	APP.5.2.M3(a)	Microsoft Exchange'i taristu süsteemide jaoks on koostatud ja **dokumenteeritud** pääsuõiguste kontseptsioon.	Store	one-off
578	E-ITS_2	APP.5.2.M7(a)	Miigreerimise etapid on hoolikalt kavandatud ja **dokumenteeritud**. Migreerimise kavas on arvestatud postkastide, objektide, turvapoliitikate, Active Directory Domain Service ülesehituse, meilisüsteemide ning Microsoft Exchange'i ja Outlooki versioonide funktsioonide erinevustega.	Store	event-based
579	E-ITS_2	APP.5.2.M7(b)	Enne installimist töökeskkonda on uut süsteemi testitud eraldi testimisvõrgus. Testimise tulemused on **dokumenteeritud**.	Store	event-based
580	E-ITS_2	APP.5.2.M9(b)	Microsoft Exchange'i konnektorite konfiguratsioon on turvaline. Konnektorite konfiguratsiooni muudatused **dokumenteeritakse**.	Store	event-based
581	E-ITS_2	APP.5.2.M11(a)	On määratud ja **dokumenteeritud**, milliste turvamehhanismidega suhtlust Microsoft Exchange'i süsteemidega kaitstakse.	Store	one-off
582	E-ITS_2	APP.5.2.M17(a)	On **dokumenteeritud** juhend PST-failide ja Managed Store'i krüpteerimiseks	Store	one-off
583	E-ITS_2	APP.5.3.M1(a)	Organisatsioon on e-posti klientidele **kehtestanud** turvalise lubatava konfiguratsiooni.	Store	one-off
584	E-ITS_2	APP.5.3.M2(d)	On **koostatud** kirjalik loend konkreetses e-posti serveris lubatud protokollidest ja teenustest.	Store	one-off
585	E-ITS_2	APP.5.3.M6(a)	Organisatsioon on **koostanud** e-posti turvaliseks kasutamiseks turvaeeskirja, mis on kooskõlas organisatsiooni infoturvapoliitikaga.	Store	one-off
586	E-ITS_2	APP.5.3.M6(e)	Haldurite tarbeks on **koostatud** täiendavad juhised, mis määratlevad: • kuidas konfigureeritakse e-posti serveri ja kliendi komponente; • kuidas toimub teiste serverite juurdepääs e-posti serverile; • millistelt töökohtadelt ja mis viisil on e-posti serveri haldus lubatud.	Store	one-off
587	E-ITS_2	APP.5.4.M1(b)	Organisatsioon on **koostanud** UCC-teenuste kasutuselevõtu kava, mis kirjeldab vähemalt järgmist: • eesmärgid, mida tahetakse UCC-teenuste kasutuselevõtuga saavutada; • funktsionaalsed nõuded (nii UCC-lahendusele tervikuna kui üksikutele teenustele); • UCC-teenustele kohalduvad infoturbe nõuded; • UCC-teenuste kaudu edastatav lubatav teave ja andmespetsifikatsioonid; • organisatsiooni nõuetele vastavate UCC-teenuste loetelu; • UCC ja teiste IT-teenuste omavahelise sõltuvuse analüüs; • muudatused organisatsiooni töökorralduses seoses UCC-teenuste kasutuselevõtuga.	Store	one-off
588	E-ITS_2	APP.5.4.M1(c)	Organisatsioon on **koostanud** juhendi UCC-komponentide integreerimiseks organisatsiooni IT-süsteemide ja IT-taristuga.	Store	one-off
589	E-ITS_2	APP.6.M1(a)	Tarkvara kasutuselevõtu kavandamise käigus on **kirjeldatud**: • tarkvara kasutamise eesmärk; • andmed, mida tarkvaraga töödeldakse; • riistvara ja IT-süsteemid, millel tarkvara kasutatakse; • tarkvara liidestus ja lõimimine olemasolevate rakendustega; • välise toe vajadus tarkvara juurutamisel ja käigushoidmisel.	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
590	E-ITS_2	APP.6.M2(a)	Tarkvara kasutuselevõtu kavandamise tulemite põhjal on **koostatud** ja kinnitatud tarkvarale esitavate nõuete loend.	Store	one-off
591	E-ITS_2	APP.6.M4(c)	Tarkvara installimiseks **koostatakse** installijuhend, mis sisaldab kõiki käsitsi tehtavaid installisamme, sh installimise käigus tehtavaid konfiguratsioonimuudatusi.	Store	one-off
592	E-ITS_2	APP.6.M4(f)	Tarkvara tüüpkonfiguratsioon ja selles tehtud muutused **dokumenteeritakse**.	Store	event-based
593	E-ITS_2	APP.6.M8(d)	Tarkvara konfiguratsioonifailidest on tehtud varukoopia, seadistamistegevused on **dokumenteeritud**.	Store	event-based
594	E-ITS_2	APP.6.M10(a)	Nõuded tarkvara turvaliseks seadistamiseks ja kasutamiseks on **koondatud** tarkvara turvajuhendisse.	Store	one-off
595	E-ITS_2	APP.6.M13(b)	Desinstallimise käigus tehtud süsteemimuudatused **dokumenteeritakse** (käsitsi või spetsiaalsete programmide abil).	Store	event-based
596	E-ITS_2	APP.7.M1(b)	Organisatsioon on **teostanud** esmase analüüsi ja määranud tellimustarkvara raamtingimused, sealhulgas: • äriprotsessid, mida rakendus toetab; • töödeldavad andmed ja nende kaitsetarve; • õiguslikud raamtingimused; • IT-süsteemid, millega rakendus andmeid vahetab; • vajalikud rollid ja pääsuõigused.	Store	one-off
597	E-ITS_2	APP.7.M1(c)	Arendusprojekti läbiviimiseks on **kinnitatud** tarkvaraarenduse metoodika ja projektijuhtimise mudel.	Store	one-off
598	E-ITS_2	APP.7.M2(a)	Organisatsioon on **kinnitanud** arendusprotsessi korralduslikud ja tehnilised turvanõuded.	Store	one-off
599	E-ITS_2	APP.7.M3(a)	IT-talitus on **koostanud** tellimustarkvara käitamiseks nõutava riist- ja tarkvara spetsifikatsiooni: • riistvaraplatvorm (sh server ja salvestusseadmed); • tarkvara (sh operatsioonisüsteem ja andmebaas); • süsteemiressursid (sh nõuded protsessorile, muutmälule ja salvestusmahule).	Store	one-off
600	E-ITS_2	APP.7.M3(b)	Tarkvara lõimimiseks teiste IT-süsteemidega on **koostatud** liidestuse spetsifikatsioon.	Store	one-off
601	E-ITS_2	APP.EE.1.M1(a)	On **läbi viidud** X-tee andmeteenuse vajaduse ning nõuete analüüs, milles käsitletakse vähemalt järgmist: • äriprotsessis või -teenuse andmevahetusvajaduste tuvastamine; • andmevahetuse kooseisus olevate andmete edastamise/vastuvõtmise/töötlemise õiguslikud alused; • isikuandmete (eelkõige isikuandmete eriliikide) olemasolu ning selliste andmete töötlemise reeglid; • andmete puhverdamise lubatavus ja ajalised piirid; • käideldavusnõuete (sh teenuse kasutamise mahud ja kasutusmustrid) määratlemine.	Store	one-off
602	E-ITS_2	APP.EE.2.M1(a)	Organisatsioon on **koostanud** ja kinnitanud organisatsiooni eesmärkide ja strateegilise arengukavaga kooskõlas oleva tehisintellektisüsteemide strateegia.	Store	one-off
603	E-ITS_2	APP.EE.2.M3(a)	On **teostatud** mõjuhinnang, kuidas AI-süsteem mõjutab äriprotsesside toimimist ja milline on AI-süsteemi turvalisuse riivest tulenev maksimaalne võimalik kahju.	Store	one-off
604	E-ITS_2	APP.EE.2.M3(e)	**Eksisteerib** tegevuskava AI-süsteemidega seotud riskide käsitlemiseks. Jääkriskid on tippjuhtkonna poolt aktsepteeritud.	Store	one-off
605	E-ITS_2	APP.EE.2.M5(b)	Organisatsioon on AI-süsteemi kavandamise käigus analüüsinud, et süsteemis kasutatavad andmed ja tarkvara ei riku intellektuaalomandi kaitset, autoriõigusi ega toodete litsentsitingimusi. Analüüsi tulem on **dokumenteeritud**.	Store	one-off
606	E-ITS_2	APP.EE.2.M6(e)	Kõik AI-süsteemi projekteerimist, arendamist, evitamist ja muutmist käsitlevad sisulised otsused **dokumenteeritakse**.	Store	event-based
607	E-ITS_2	APP.EE.2.M8(f)	Organisatsioon on **koostanud** andmesõnastiku (ingl data dictionary) ja dokumenteerinud metaandmete ning erinevate andmetüüpide salvestamise, vormindamise ja taasesitamise reeglid.	Store	one-off
608	E-ITS_2	APP.EE.2.M10(a)	AI-mudeli treenimise ja testimise meetodid (nt A/B testimine), testistsenaariumid ja testitulemused on **dokumenteeritud**.	Store	one-off
609	E-ITS_2	APP.EE.2.M11(a)	AI-mudeli arhitektuur ja treenimiseks kasutatavad andmeallikad (ingl data source) ning hüperparameetrid on **dokumenteeritud** ja valideeritud.	Store	one-off
610	E-ITS_2	APP.EE.2.M11(b)	Andmevalimite koostamise (ingl data sampling) ja andmete eeltöötluse (nt andmete puhastamise ja normaliseerimise) meetodid ja protsessid on **dokumenteeritud**.	Store	one-off
611	E-ITS_2	APP.EE.2.M12(a)	Tulenevalt eelnevalt läbi viidud mõjuanalüüsist (APP.EE.2.M3 AI-süsteemi riskide kaalutlemine ja mõjuhinnangu läbiviimine) on **koostatud** tegevuskava AI-süsteemi tulemuste õigsuse ja läbipaistvuse regulaarseks hindamiseks.	Store	one-off
612	E-ITS_2	APP.EE.2.M14(a)	**Eksisteerivad** juhendid AI-süsteemiga seotud intsidentide avastamiseks, nendest teavitamiseks, intsidentide lahendamiseks ja eskaleerimiseks.	Store	one-off
613	E-ITS_2	APP.EE.2.M14(d)	AI-süsteemidega seotud intsidendid **dokumenteeritakse** hilisema analüüsi tarbeks.	Store	event-based
614	E-ITS_2	IND.1.M4(a)	Käidutehnoloogia taristu halduseks on **koostatud** täielik, ajakohane ja praktiliselt kasutatav dokumentatsioon, sh varade loend.	Store	one-off
615	E-ITS_2	IND.1.M6(a)	Organisatsioonis on määratletud, **dokumenteeritud** ja rakendatud käidu- ja protsessijuhtimissüsteemide muudatuste läbiviimise protsess.	Store	one-off
616	E-ITS_2	IND.1.M7(d)	Õiguste seis ja õiguste ajalugu on läbivaatuskõlblikult **dokumenteeritud**.	Store	event-based
617	E-ITS_2	IND.1.M8(a)	Käidutehnoloogia komponentide esmaseks konfigureerimiseks on **koostatud** kontroll-loend, mis sõltuvalt komponendist määrab: • tarbetute või ebaturvaliste funktsioonide, liideste jm elementide desaktiveerimise; • turvafunktsioonide aktiveerimise; • pääsu reguleerimise ja autentimise; • algparoolide asendamise; • kaugpääsu ja kaughoolduse; • aja sünkroniseerimise; • logimise.	Store	one-off
618	E-ITS_2	IND.1.M8(f)	Kaughooldus- ja haldustoimingute volitamine, järelevalve ja juhtimine toimub reguleeritult. Juurdepääs kaughoolduseks aktiveeritakse ainult konkreetseks kasutuskorraks ja pärast seda uuesti desaktiveeritakse. Hooldustoimingud **dokumenteeritakse**.	Store	event-based
619	E-ITS_2	IND.1.M9(a)	On **kehtestatud** käidutehnoloogia valdkonna ird-andmekandjate ja mobiilseadmete kasutamise eeskiri.	Store	one-off
620	E-ITS_2	IND.1.M10(a)	Organisatsioonis on **kehtestatud** käidu- ja protsessijuhtimissüsteemide logi- ja sündmustehalduse protseduur, mis sisaldab turvasündmuste tuvastamise ja nendest teavitamise meetmeid ning intsidentide käsitlemise plaani.	Store	one-off
621	E-ITS_2	IND.1.M11(a)	Käidu -ja protsessijuhtimissüsteemide hankimiseks, arendamiseks ja integreerimiseks on **kehtestatud** ja dokumenteeritud vajalikul kaitsetarbel põhinevad ühilduvus-, töökindlus- ja turvanõuded. Need nõudeid käsitletakse osana pakkumiskutse dokumentidest.	Store	one-off

IO-ID	Act	REF	Obligation	Obligation Type	Frequency
622	E-ITS_2	IND.1.M11(c)	Lepingupartneritega (arendajad, tarnijad või organisatsioonivälised käitajad) on **sõlmitud** konfidentsiaalsuslepped.	Store	event-based
623	E-ITS_2	IND.1.M12(a)	Käidu -ja protsessijuhtimissüsteemide turvalisuse tagamiseks on **kehtestatud** nõrkuste halduse kord. Kord käsitleb käidutehnoloogia komponentide tarkvara, protokollide ja väliste liideste nõrkuste tuvastamist ja edasiste tegevuste kavandamist.	Store	one-off
624	E-ITS_2	IND.1.M20(a)	Käidu- ja protsessijuhtimissüsteemid on **dokumenteeritud** nende kasutamiseks ja haldamiseks piisava detailsusega.	Store	one-off
625	E-ITS_2	IND.1.M21(a)	Tööstusautomaatika komponentide andmevahetuspartnerid, andmekategooriad ja andmevahetuse tehniline spetsifikatsioon on **dokumenteeritud**.	Store	one-off
626	E-ITS_2	IND.1.M13(a)	Iga turvatsooni kohta on **kehtestatud** ja dokumenteeritud avariikäsitluse plaan (vt moodul DER.4 Avariihaldus), mis arvestab vähemalt järgmiste avariistsenaariumitega: • internetiühenduse pikaajaline (üle ühe nädala) katkestus; • kontori-IT täielik väljalangemine teatud ajaks (nt 2 päeva); • käidutehnoloogia elutähtsate IT-komponentide ajutine väljalangemine; • käidutehnoloogia elutähtsate IT-komponentide turvarike ründe või kahjurprogrammi tõttu.	Store	one-off
627	E-ITS_2	IND.1.M13(b)	Käidu- ja protsessijuhtimissüsteemide jaoks on **välja töötatud** varundamise ja taastamise kord, milles esitatakse: • varundamise, taastamise ja varukoopiate regulaarse testimise protseduurid; • süsteemide taastamise protseduurid; • defektsete komponentide parandamine; • varuosade vajadus ning hoidmine; • alternatiivsed side- ja juhtimisvõimalused tõrgete korral.	Store	one-off
628	E-ITS_2	IND.1.M14(e)	Autentimissüsteemide konfiguratsioon ja muudatused **dokumenteeritakse** ning süsteeme kontrollitakse intsidentide avastamiseks.	Store	event-based
629	E-ITS_2	IND.1.M15(a)	Organisatsioon on **koostanud** varade ülevaate, mis sisaldab kõigi oluliste käidu- ja protsessijuhtimissüsteemide pääsuõiguste hetkeseisu ja muutmise ajalugu (vt IND.1.M7 Keskne õiguste haldus).	Store	one-off
630	E-ITS_2	IND.1.M17(a)	Käidutehnoloogia komponentide turbe kontseptsiooni vastavust turvapoliitikale ja komponentide konfiguratsiooni asjakohasust vaadatakse läbi perioodiliselt ja/või vastavalt vajadusele, näiteks uute ohtude ilmnemisel.	Update	periodic; event-based
631	E-ITS_2	IND.2.1.M1(c)	Tööstusautomaatika komponentide konfiguratsiooni saab muuta selleks volitatud ja autenditud töötaja. Konfiguratsioonimuudatused **dokumenteeritakse**.	Store	event-based
632	E-ITS_2	IND.2.1.M6(b)	Tööstusautomaatika komponentide töö sõltuvused võrguteenustest on **dokumenteeritud**.	Store	event-based
633	E-ITS_2	IND.2.1.M19(c)	Testimistulemused **dokumenteeritakse**, tuvastatud riske analüüsitakse ja käsitletakse.	Store	event-based
634	E-ITS_2	IND.2.2.M1(b)	Konfiguratsioonimuudatused ja komponentide väljavahetamine **dokumenteeritakse**.	Store	event-based
635	E-ITS_2	IND.2.3.M2(a)	Andureid kalibreeritakse regulaarselt, kalibreerimine **dokumenteeritakse**.	Store	event-based
636	E-ITS_2	IND.2.4.M1(a)	On **kehtestatud** keskne kaughalduse eeskiri, mis määrab, milliseid kaughoolduslahendusi kasutatakse, kuidas kaitstakse sideühendusi ja tehakse kaughoolduse seiret.	Store	one-off
637	E-ITS_2	IND.2.4.M2(a)	On **kehtestatud** protseduur robotseadme turvaliseks käituseks pärast garantiiaja lõppu.	Store	one-off
638	E-ITS_2	IND.2.7.M1(a)	Ohutusautomaatika süsteemidesse kuuluvad riist- ja tarkvarakomponendid, andmed ja ühendused on **dokumenteeritud**.	Store	event-based
639	E-ITS_2	IND.2.7.M5(a)	On **kehtestatud** ohutusautomaatika intsidendikäsitlusplaan, mis määrab vajalikud rollid ja kohustused.	Store	one-off
640	E-ITS_2	IND.2.7.M11(a)	On **välja töötatud** strateegia ohutusega seotud komponentide kasutamiseks integreeritud süsteemides.	Store; Update	one-off
641	E-ITS_2	IND.3.2.M1(a)	On **kehtestatud** organisatsiooniülene kord käidutehnoloogia (ingl operational technology, OT) komponentide kaughoolduse tellimiseks ja läbiviimiseks.	Store	one-off
642	E-ITS_2	IND.3.2.M1(d)	Kõik kaughoolduseks kasutatavad tehnilised lahendused on keskselt **dokumenteeritud**.	Store; Update	event-based
643	E-ITS_2	IND.3.2.M2(b)	Kaughoolduse juurdepääsuõigused on **dokumenteeritud**. Dokumenteerimine on korraldatud analoogiliselt arvutivõrgu IT-süsteemide kaugjuurdepääsude dokumenteerimisega.	Store	event-based
644	E-ITS_2	IND.3.2.M3(b)	On **kehtestatud** protseduurid käidutehnoloogia kaughoolduse korrast erandite heakskiitmiseks ja kinnitamiseks	Store	one-off
645	E-ITS_2	IND.3.2.M9(a)	Turvaliseks failivahetuseks OT kaughoolduse käigus (nt. konfiguratsioonifailide, süsteemiuuendite või juhendite saatmiseks) on **kehtestatud** turvameetmeid sisaldavad protseduurid.	Store	one-off

Appendix 4 – Named documentary requirements identified in the regulatory texts

IO-ID	Act	REF	Document type	Document name
041	E-ITS_1	6.1	policy document	Infoturvapoliitika
043	E-ITS_1	6.1.7	policy document	Infoturvapoliitika
044	E-ITS_1	6.2.3(a)	register / inventory / list	Äriprotsesside register
045	E-ITS_1	6.2.3(a)	register / inventory / list	Varade register
045-1	E-ITS_1	6.2.3(b)	policy document	Kaitseala kirjeldus
045-2	E-ITS_1	6.2.3(d)	record	Turbeprotsessi klassifikaatorid
046	E-ITS_1	6.2.3(e)	policy document	Infoturvaeesmärgid
047	E-ITS_1	6.2.4	policy document	Infoturvaeesmärgid
049	E-ITS_1	6.7.2	policy document	Dokumendihalduskord
068	E-ITS_3	5.4.8	report	IT riskianalüüs
069	E-ITS_3	5.4.9	plan	Infoturbe meetmete rakendusplaan
076	E-ITS_3	9.3	report	E-ITS eelauditi aruanne
077	E-ITS_3	10.2	plan	E-ITS auditi plaan
078	E-ITS_3	10.11	report	E-ITS põhiauditi lõpparuanne
080	E-ITS_3	11.5	report	E-ITS vaheauditi aruanne
082	E-ITS_3	12.13	report	E-ITS auditi aruande kavand
085	E-ITS_3	13.4	report	E-ITS järelauditi aruanne
088	KTN_1	1.2	policy document	Võrgu- ja infosüsteemide turvareeglid
092	KTN_1	3.2	policy document	Andmete kasutamise reeglid
096	KTN_1	8.1	documentation	Arvutivõrgu skeem
100	E-ITS_2	ISMS.1.M3(b)	policy document	Infoturvapoliitika
102	E-ITS_2	ISMS.1.M3(f)	policy document	Infoturvapoliitika
104	E-ITS_2	ISMS.1.M6(a)	policy document	Infoturbe korraldus
109	E-ITS_2	ISMS.1.M10(a)	concept document	Turbekontseptsioon; Infoturbe strateegia
116	E-ITS_2	ISMS.1.M13(b)	policy document	Dokumendihalduskord
121	E-ITS_2	ORP.1.M16(a)	policy document	IT-vahendite turvalise kasutamise eeskiri
123	E-ITS_2	ORP.1.M16(e)	policy document	IT-vahendite turvalise kasutamise eeskiri
129	E-ITS_2	ORP.3.M3(c)	policy document	IT-, tööstusautomaatika ja esemevõrgu komponentide turvalise kasutamise eeskiri
131	E-ITS_2	ORP.4.M1(a)	policy document	Kasutajakontode halduse eeskiri
136	E-ITS_2	ORP.4.M8(a)	policy document	Paroolide kasutamise kord
136-1	E-ITS_2	ORP.4.M12(a)	policy document	Autentimiskord
141	E-ITS_2	CON.1.M4(a)	policy document	Krüptovõtmete võtmehalduse kord
142	E-ITS_2	CON.1.M10(a)	concept document	Krüptokontseptsioon
143	E-ITS_2	CON.1.M19(a)	register / inventory / list	Krüptograafiliste vahendite loend
147	E-ITS_2	CON.2.M4(a)	guideline; policy document	Andmekaitsepoliitika; Andmekaitsejuhised
148	E-ITS_2	CON.2.M7(a)	policy document	Andmekaitsetingimused
153	E-ITS_2	CON.2.M16(a)	guideline	Isikuandme töötlemise eeskiri
159	E-ITS_2	CON.2.M25(a)	policy document	Isikuandme töötlemise eeskiri
163	E-ITS_2	CON.3.M6(a)	concept document	Andmevarunduse kontseptsioon
165	E-ITS_2	CON.6.M1(a)	policy document	Andmete kustutuse ja hävitamise kord
167	E-ITS_2	CON.7.M1(a)	policy document	Välislähetuste infoturbe eeskiri
171	E-ITS_2	CON.8.M5(b)	policy document	Tarkvarasüsteemide kavandamise reeglid
172	E-ITS_2	CON.8.M11(a)	policy document	Tarkvaraarenduste läbiviimise kord
174	E-ITS_2	CON.9.M2(a)	policy document	Teabevahetuse kord
175	E-ITS_2	CON.9.M2(b)	guideline	Kaitsetarbe määramise juhised
195	E-ITS_2	OPS.1.1.2.M20(d)	register / inventory / list	Varade register
197	E-ITS_2	OPS.1.1.3.M1(a)	policy document	Paiga- ja muudatusehalduse kord
202	E-ITS_2	OPS.1.1.3.M11(b)	policy document	IT-süsteemides muudatuste dokumenteerimise kord
204	E-ITS_2	OPS.1.1.4.M1(a)	concept document	IT-süsteemide kahjurprogrammide kaitse kontseptsioon
206	E-ITS_2	OPS.1.1.4.M9(d)	plan	Kahjurprogrammide eeldamise ja nakatuseelse olukorra taastamise tegevuskava
207	E-ITS_2	OPS.1.1.5.M1(a)	policy document	Logimise eeskiri
212	E-ITS_2	OPS.1.1.6.M10(b)	policy document	Testimise vastuvõtu kord
217	E-ITS_2	OPS.1.1.7.M1(b)	requirements	Süsteemihalduse taristu tehnilised nõuded
218	E-ITS_2	OPS.1.1.7.M2(a)	requirements	Süsteemihalduse nõuded
220	E-ITS_2	OPS.1.1.7.M7(a)	policy document	Süsteemihalduse turvaeeskiri
221	E-ITS_2	OPS.1.1.7.M7(d)	record	Süsteemihalduse turvaeeskiri
222	E-ITS_2	OPS.1.1.7.M8(a)	concept document	Süsteemihalduse kontseptsioon
227	E-ITS_2	OPS.1.2.2.M1(c)	policy document	Elektroonilise arhiveerimise konfidentsiaalsus-, terviklus-, käideldavus- ja autentsusnõuded
228	E-ITS_2	OPS.1.2.2.M2(a)	concept document	Arhiveerimiskontseptsioon

IO-ID	Act	REF	Document type	Document name
229	E-ITS_2	OPS.1.2.2.M10(a)	policy document	Arhiivisüsteemi kasutamise eeskiri
234	E-ITS_2	OPS.1.2.4.M1(a)	policy document	Kaugtöö eeskiri
236	E-ITS_2	OPS.1.2.4.M1(d)	policy document	Kaugtöö eeskiri
237	E-ITS_2	OPS.1.2.4.M6(a)	concept document	Kaugtöö turbekontseptsioon
238	E-ITS_2	OPS.1.2.4.M6(d)	concept document	Kaugtöö turbekontseptsioon
243	E-ITS_2	OPS.2.2.M1(a)	strategy document	Pilvteenuste strateegia
246	E-ITS_2	OPS.2.2.M2(a)	policy document	Pilvteenuste turvapoliitika
250	E-ITS_2	OPS.2.2.M5(a)	plan	Pilvteenusele migreerimise kava
254	E-ITS_2	OPS.2.3.M1(a)	policy document	Väljasttellitavate teenuste turvanõuded
257	E-ITS_2	OPS.2.3.M8(a)	strategy document	Väljasttellimise strateegia
258	E-ITS_2	OPS.2.3.M9(a)	policy document	Hankepoliitika
264	E-ITS_2	OPS.3.2.M5(a)	concept document	Turvakontseptsioon
272	E-ITS_2	DER.1.M1(a)	policy document	Turvaintsidentide avastamise eeskiri
274	E-ITS_2	DER.1.M2(a)	guideline	Logiandmete analüüsile kohaldatavate õigusaktide nõuded
275	E-ITS_2	DER.1.M3(a)	policy document	Turvasündmustest teavitamise kord
276	E-ITS_2	DER.1.M6(b)	guideline	Logiandmete analüüsi juhend
278	E-ITS_2	DER.2.1.M2(a)	guideline	Turvaintsidentide käsitluse juhend
281	E-ITS_2	DER.2.1.M9(a)	guideline	Turvaintsidentidest teavitamise juhend
282	E-ITS_2	DER.2.1.M10(b)	plan	Intsidendi käsitlemise tegevuskava
284	E-ITS_2	DER.2.1.M14(a)	documented procedure	Turvaintsidentidest teavitamise eskalatsiooniplaan
285	E-ITS_2	DER.2.2.M5(a)	guideline	Asitõendite turbe juhend
298	E-ITS_2	DER.3.2.M2(a)	guideline	Auditite läbiviimise juhend
299	E-ITS_2	DER.3.2.M4(c)	plan	Auditikava
300	E-ITS_2	DER.4.M1(a)	guideline	Avariiteatmik
301	E-ITS_2	DER.4.M3(a)	strategy document	Avariihalduse strateegia
302	E-ITS_2	DER.4.M4(a)	policy document	Avariihalduse poliitika
303	E-ITS_2	DER.4.M8(a)	plan	Avariihalduse teadvustus- ja koolituskava
308	E-ITS_2	INF.1.M9(a)	documentation	Hoonete turbe programm
324	E-ITS_2	INF.7.M5(d)	policy document	Kuvariga töötamise kord
325	E-ITS_2	INF.8.M2(a)	policy document	Dokumentide ja andmekandjate käitlemise kord
326	E-ITS_2	INF.8.M5(a)	guideline	Konfidentsiaalsete andmete kõrvaldamise kord
327	E-ITS_2	INF.9.M1(a)	policy document	Mobiilseadmete kasutamise eeskiri
328	E-ITS_2	INF.9.M4(a)	policy document	Organisatsioonivälise IT-süsteemide tööalase kasutamise kord
330	E-ITS_2	INF.10.M1(a)	policy document	Ruumide kasutamise kord
333	E-ITS_2	INF.11.M3(e)	guideline	Sõiduki IT-süsteemide turvalise kasutamise ja haldamise juhend
334	E-ITS_2	INF.11.M4(b)	policy document	Sõidukite infoturbe eeskiri
336	E-ITS_2	INF.11.M6(a)	guideline	Sõiduki avariiolukorra või IT-komponentide rikke tegevusjuhised
337	E-ITS_2	INF.11.M6(c)	guideline	Sõiduk ärandamise või volitamata sissetungi tegevusjuhend
338	E-ITS_2	INF.11.M7(a)	policy document	Sõidukite kasutamise kord
339	E-ITS_2	INF.11.M11(a)	guideline	Sõiduki ootamatu rikke tegevuskava
343	E-ITS_2	INF.12.M13(b)	policy document	Isiklike elektriseadmete kasutamise kord
351	E-ITS_2	INF.13.M4(a)	policy document	Hoonete tehnilise halduse turvaeeskiri
352	E-ITS_2	INF.13.M6(a)	concept document	Hoonete tehnilise halduse kontseptsioon
353	E-ITS_2	INF.13.M6(c)	concept document	Hoonete tehnilise halduse kontseptsioon
362	E-ITS_2	INF.13.M26(a)	policy document	BIM juurutamise ja käitamise turvameetmed
366	E-ITS_2	INF.14.M7(a)	policy document	Hooneautomaatikasüsteemi turvaeeskiri
368	E-ITS_2	INF.14.M9(a)	concept document	Hooneautomaatikasüsteemi kontseptsioon
370	E-ITS_2	INF.14.M27(c)	plan	Hooneautomaatika avariihalduse tegevuskava
372	E-ITS_2	NET.1.1.M1(a)	policy document	Võrgu turvapoliitika
379	E-ITS_2	NET.1.1.M22(a)	policy document	Võrgu segmentimise eeskiri
385	E-ITS_2	NET.1.2.M13(a)	concept document	Võrguhalduse kontseptsioon
386	E-ITS_2	NET.1.2.M14(a)	plan	Võrguhalduse rakendusplaan
387	E-ITS_2	NET.1.2.M15(a)	policy document	Võrguhalduse taristu turvalise kasutamise kord
390	E-ITS_2	NET.2.1.M8(a)	policy document	Raadiovõrgu intsidentide käsitlemise kord
391	E-ITS_2	NET.2.1.M10(a)	policy document	Raadiokohtvõrgu turvajuhend
396	E-ITS_2	NET.2.2.M1(a)	policy document	Raadikohtvõrgu kasutamise eeskiri
399	E-ITS_2	NET.3.1.M10(a)	policy document	Ruuterite ja kommutaatorite turvajuhend
404	E-ITS_2	NET.3.2.M1(a)	policy document	Tulemüüride turvajuhend
413	E-ITS_2	NET.3.3.M8(a)	guideline	Virtuaalse privaatvõrgu turvalise kasutamise juhend
414	E-ITS_2	NET.3.3.M10(a)	policy document	Virtuaalse privaatvõrgu turvalise käituse põhimõtted
420	E-ITS_2	NET.4.1.M6(a)	guideline	Telefonikeskjaama turvajuhend
423	E-ITS_2	NET.4.2.M1(a)	plan	Sidesüsteemi kasutuselevõtu kava
426	E-ITS_2	NET.4.2.M7(a)	guideline	Sidesüsteemi turvajuhend
430	E-ITS_2	SYS.1.1.M10(a)	policy document	Serverite logimise kord
431	E-ITS_2	SYS.1.1.M11(a)	guideline	Serveri turvajuhend
436	E-ITS_2	SYS.1.1.M22(c)	plan	Serveriteenuste taastekava
440	E-ITS_2	SYS.1.1.M27(d)	policy document	Anomaaliate teavitamise ja käsitlemise kord
450	E-ITS_2	SYS.1.6.M10(b)	guideline	Konteinerite käitamise eeskiri
452	E-ITS_2	SYS.1.6.M21(a)	guideline	Konteinerite pääsuõiguse haldamise eeskiri
453	E-ITS_2	SYS.1.8.M6(a)	policy document	Salvestilahenduse turvajuhend
455	E-ITS_2	SYS.1.8.M7(b)	plan	Salvestilahenduse rakendamise kava

IO-ID	Act	REF	Document type	Document name
458	E-ITS_2	SYS.1.8.M10(a)	guideline	Salvestilahenduse käitamise juhend
465	E-ITS_2	SYS.1.8.M18(a)	guideline	Salvestisüsteemide läbivaatuse kord
466	E-ITS_2	SYS.1.8.M20(a)	guideline	Salvestilahenduse avariikava
467	E-ITS_2	SYS.1.9.M1(a)	policy document	Terminalserveri turvanõuded
471	E-ITS_2	SYS.2.1.M9(a)	guideline	Klientarvuti turvalise kasutamise juhend
474	E-ITS_2	SYS.2.1.M10(a)	plan	Klientarvutite kasutuselevõtu kava
478	E-ITS_2	SYS.2.1.M20(a)	guideline	Klientarvuti tavapäraste haldustööde haldusjuhis
479	E-ITS_2	SYS.2.1.M21(a)	policy document	Kaamera ja mikrofoni kasutamise kord
490	E-ITS_2	SYS.3.1.M1(a)	policy document	Sülearvutite mobiilse kasutamise kord
492	E-ITS_2	SYS.3.1.M6(a)	policy document	Sülearvuti kasutamise eeskiri
495	E-ITS_2	SYS.3.2.1.M1(a)	policy document	Nutitelefonide ja tahvelarvutite kasutamise eeskiri
496	E-ITS_2	SYS.3.2.1.M2(a)	policy document	Nutitelefonide ja tahvelarvutite pilvekasutuse kord
498	E-ITS_2	SYS.3.2.1.M10(a)	guideline	Nutitelefonide ja tahvelarvutite keskse halduse juhend
499	E-ITS_2	SYS.3.2.1.M31(a)	policy document	Mobiilmaksete kord
503	E-ITS_2	SYS.3.2.3.M10(b)	guideline	Biomeetrilise autentimise juhend
507	E-ITS_2	SYS.4.1.M1(a)	plan	Printerite ja kontorikombainide rakendamise kava
509	E-ITS_2	SYS.4.1.M5(a)	guideline	Printerite ja kontorikombainide turvalise käsitsemise turvaeeskiri
510	E-ITS_2	SYS.4.1.M22(a)	policy document	Tarbetute tundlikku teavet sisaldavate dokumentide hävitamise kord
511	E-ITS_2	SYS.4.1.M4(a)	policy document	Printerite ja kontorikombainide turvaeeskiri
513	E-ITS_2	SYS.4.3.M1(c)	policy document	Sardsüsteemide tervikluse ja töövõimelisuse testimise kord
517	E-ITS_2	SYS.4.3.M16(d)	guideline	Muukimisintsidentidele reageerimise juhend
524	E-ITS_2	SYS.4.5.M4(a)	policy document	Irdandmekandjate kasutamise eeskiri
525	E-ITS_2	SYS.4.5.M5(a)	policy document	Irdandmekandjate väljaviimise kord
526	E-ITS_2	SYS.4.5.M6(a)	policy document	Irdandmekandjate haldamise kord
527	E-ITS_2	SYS.4.5.M7(b)	guideline	Andmete turvalise kustutamise juhend
528	E-ITS_2	SYS.EE.1.M21(a)	requirements	Turvaserveri teenuse standardtingimused
535	E-ITS_2	APP.2.1.M1(a)	policy document	Kataloogiteenuste turvaeeskiri
541	E-ITS_2	APP.2.1.M16(a)	plan	Kataloogiteenuse avariikava
542	E-ITS_2	APP.2.2.M1(b)	policy document; concept document	AD õiguste kontseptsioon; Õiguste delegeerimise kord
553	E-ITS_2	APP.3.2.M9(a)	policy document	Veebiserveri turvapoliitika
561	E-ITS_2	APP.4.3.M1(a)	policy document	Andmebaasisüsteemide turvaeeskiri
577	E-ITS_2	APP.5.2.M3(a)	concept document	Microsoft Exchange pääsuõiguste kontseptsioon
585	E-ITS_2	APP.5.3.M6(a)	policy document	E-posti turvalise kasutamise eeskiri
598	E-ITS_2	APP.7.M2(a)	policy document	Tarkvara arendusprotsessi turvanõuded
602	E-ITS_2	APP.EE.2.M1(a)	strategy document	Tehisintellektisüsteemide strateegia
619	E-ITS_2	IND.1.M9(a)	policy document	Käidutehnoloogia valdkonna ird-andmekandjate ja mobiilseadmete kasutamise eeskiri
620	E-ITS_2	IND.1.M10(a)	policy document	Käidu- ja protsessijuhtimissüsteemide logi- ja sündmustehalduse kord
621	E-ITS_2	IND.1.M11(a)	requirements	Käidu- ja protsessijuhtimissüsteemide turvanõuded
623	E-ITS_2	IND.1.M12(a)	policy document	Käidu- ja protsessijuhtimissüsteemide nõrkuse haldamise kord
627	E-ITS_2	IND.1.M13(b)	policy document	Käidu- ja protsessijuhtimissüsteemide varundamise ja taastamise kord
630	E-ITS_2	IND.1.M17(a)	concept document	Käidutehnoloogia komponentide turbe kontseptsioon
636	E-ITS_2	IND.2.4.M1(a)	policy document	Kaughalduse eeskiri
639	E-ITS_2	IND.2.7.M5(a)	plan	Ohutusautomaatika intsidendikäsitlusplaan
640	E-ITS_2	IND.2.7.M11(a)	strategy document	Ohutuskomponentide kasutamine integreeritud süsteemides

Appendix 5 – Comparison with the E-ITS guidance sample-document list

Nr in E-ITS sample docs	Name in E-ITS sample docs	Name in Acts	Reference
N01	Infoturvapoliitika	Infoturvapoliitika	ISMS.1.M3(b)
N01.1	Infoturvaeesmärgid	Infoturvaeesmärgid	E-ITS_1 6.2.3(e)
N01.2	Infoturbe strateegia	Infoturbe strateegia	No direct reference
N02	Infoturbeprotsessi kontseptsioon (turbekontseptsioon)	Turbekontseptsioon	ISMS.1.M10(a)
N03	Varade loetelu (ja nende omavahelised seosed)	Varade register	E-ITS_16.2.3(a)
N04	Ebatraditsiooniliste varade loetelu	Varade register	OPS.1.1.2.M20(d)
N05	Infoturbe aluskomponentide valik		No direct reference
N06	Turbeprotsessiks vajalikud klassifikaatorid	Turbeprotsessiks vajalikud klassifikaatorid	E-ITS_1 6.2.3(d)
N07	Kaitseala kirjeldus	Kaitseala kirjeldus	E-ITS_1 6.2.3(b)
N08	Infoturbe korraldusstruktuuri kirjeldus	Infoturbe korraldus	ISMS.1.M6(a)
N09	Tööprotseduurid ja organisatsiooni eeskirjad	-	General documentation
N10	Autentimispoliitika	Autentimiskord	ORP.4.M12(a)
N11	Turvaintsidentide avastamise korraldus (avastamine, reageerimine)	Turvaintsidentide käsitluse juhend	DER.2.1.M2(a)
N12	Võrguskeem	Arvutivõrgu skeem	KTN_1 8.1
T01	Turvapoliitika teostamise etapiline tegevusplaan.		No direct reference
T02	Turbekontseptsiooni rakendusplaan.		No direct reference
T03	Moodulite kinnis(ta)tus sihtobjektidele		General documentation
T04	Turvameetmete teostusjärjestus		No direct reference
T05	Rakendusplaani järelevalve kava		No direct reference
T06	Iga üksiku (arvelevõetud) äriprotsessi üksikasjad.	Äriprotsesside register	6.2.3(a)
T07	Turbeprotsessi käigus tehtud otsused.		General documentation
T08	Olulised lepingud partnerite ja klientidega		General documentation
T09	Juhtkonnale kommunikeeritud infoturvateave	-	ISMS.1.M12(a)
T10	Infoturbe ja turbeprotsessi kohta tehtud otsused (sh juhtkonnatasemel)	-	ISMS.1.M13(a)
T11	Infoturvameetmete nimekiri		General documentation
T12	Infoturbe (seisu) ülevaatus		No direct reference
T13	Kontrollide (nii sisemiste kui välimiste) tulemused		General documentation
T14	Infoturva intsidentide nimekiri ja lahendamise materjalid		General documentation
T15	Kasutajaõigused		General documentation
T16	Muudatustehalduse sündmused		General documentation
T17	Andmekandjate inventuur	Varade register	OPS.1.1.2.M20(d)
T18	Väliste teenuseandjate ja -tarnijate pädevustunnistused ja sertifikaadid		General documentation
T19	Talitluspidevuse käsiraamatud		General documentation
T20	Krüptograafilised võtmed ja sertifikaadid	Krüptograafiliste vahendite loend	CON.1.M4(a), CON.1.M19(a)
T21	Krüptograafilised algoritmid		No direct reference
T22	Äriprotsessidele kaitsetarbe kinnitamise akt	-	E-ITS_1 6.2.3(d)
T23	Alluvatele varadele ja ressurssidele kaitsetarbe omistamise akt	-	E-ITS_1 6.2.3(d)
T24	Kontrolljälg, logid		General documentation