TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Andres Pelešev 212086IVCM

Cybersecurity Regulatory Challenges in Small Modular Reactor Implementation: A Case Study of Estonia

Master's thesis

Supervisor: Silvia Lips
PhD

Co-supervisor: Shaymaa Mamdouh Khalil
MSc

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Andres Pelešev 212086IVCM

Küberturbe regulatiivsed väljakutsed väikemoodulreaktorite rakendamisel: Eesti juhtumiuuring

Magistritöö

Juhendaja: Silvia Lips
PhD
Kaasjuhendaja: Shaymaa Mamdouh Khalil
MSc

Tallinn 2025

Author's declaration of originality

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

Author: Andres Pelešev

15.05.2025

Abstract

Estonia has started planning its first Nuclear Power Plant (NPP) utilizing Small Modular Reactor (SMR) technology to address a growing demand for dispatchable and low-carbon electricity. Having no nuclear energy background, Estonia needs to create an entirely new nuclear regulatory framework, including cybersecurity (CS) governance tailored to its national context, shaped by evolving cyber threats, and institutional readiness.

The novelty of SMR technology introduces cybersecurity challenges that differ from those in conventional NPPs. Key issues include larger cyber-attack surfaces, increased supply chain risks due to vendor dependency, and the need to integrate cybersecurity-by-design throughout the system lifecycle. This study identifies and evaluates international cybersecurity standards, guidelines, and regulatory guides to determine their suitability as a foundational cybersecurity framework for Estonia's SMR program. The analysis considers the country's institutional capacity, cyber-threat landscape, and legislative readiness, offering a strategic model for regulatory adaptation.

The research employs an exploratory case study methodology, integrating qualitative data collection, thematic analysis of expert interviews, and structured document analysis. A context-aware evaluation approach was applied to score selected cybersecurity standards and guidelines against Estonia-specific criteria. The findings inform a phased regulatory strategy for SMR program cybersecurity governance in Estonia, recommending the adaptation of IEC 62645, IAEA NSS 17-T, STUK YVL A.12, and ISO/IEC 27001. Methodological triangulation, drawing from expert interviews, literature review, and secondary data sources, was used to validate the final outcomes against Estonia's institutional needs and experts' insight. The research provides tailored and context-aware recommendations for cybersecurity governance in the national nuclear program and contributes to the broader discourse on regulatory design for emerging nuclear nations.

This thesis is written in English and is 76 pages long, including 9 chapters, 4 figures, and 7 tables.
Keywords: cybersecurity, framework, standard, SMR, small modular reactor, nuclear power plant

Annotatsioon

Küberturbe regulatiivsed väljakutsed väikemoodulreaktorite rakendamisel: Eesti juhtumiuuring

Eesti on kavandamas oma esimest tuumaelektrijaama väikemoodulreaktori (SMR) tehnoloogial, et tagada vajalikus koguses juhitava ja süsisinikuneutraalse elektrienergia tootmine. Kuna Eestil puudub varasem tuumaenergeetika taust, tuleb selleks luua tuumaenergia regulatiivne raamistik mis käsitleb ka küberturbe regulatsioone.

SMR tehnoloogia uudsusega kaasnevad mitmed küberturbealasesd väljakutsed. Olulisemateks probleemideks on laiem küberründe pind, suurenenud tarneahela riskid ning vajadus integreerida küberturvalisus kavandatava süsteemi elutsüklisse alates disainist. Käesolevas uurimustöös vaadeldakse ja hinnatakse rahvusvahelisi küberturbe standardeid, juhiseid ja regulatiivseid suuniseid, et tuvastada kõige sobivamad, mille alusel luua Eesti SMR programmi küberturberaamistik. Analüüsis võetakse arvesse Eesti institutsionaalset võimekust, küberohtude maastikku ja seadusandlikku valmisolekut, pakkudes strateegilist mudelit regulatiivseks kohandamiseks.

Uurimistöö metoodikaks on juhtumiuuring, mis ühendab kvalitatiivse andmekogumise, ekspertintervjuude temaatilise analüüsi ning standardi- ja juhenddokumentide analüüsi. Valitud küberturbe standardite hindamiseks rakendati konteksti arvestavat hindamismeetodit, Eesti spetsiifikale vastavate kriteeriumide alusel. Tulemused näitavad, et Eestile sobib etapiviisiline regulatsioonide juurutamine ning erinevat liiki juhiste kombineerimine, põhinedes standarditel IEC 62645, IAEA NSS 17-T, STUK YVL A.12 ja ISO/IEC 27001. Metodoloogiline triangulatsioon, mis põhines ekspertintervjuudel, kirjanduse ülevaatel ja teisestel andmeallikatel, võimaldas lõppjäreldusi valideerida Eesti vajadustest lähtuvalt ja ekspertide sisendi põhjal. Uurimistöö pakub kohandatud ja kontekstitundlikke soovitusi tuumaprogrammi küberturbe korraldamiseks ning annab panuse laiemasse arutelusse alustavate tuumariikide regulatiivse raamistiku loomisel.

Magistritöö on kirjutatud inglise keeles, sisaldab 76 lehekülge, 9 peatükki, 4 joonist ja 7 tabelit.

List of abbreviations and terms

BWRX-300	Boiling Water Reactor, Generation X-300
C-SCRM	Cybersecurity Supply Chain Risk Management
CERT-EE	Estonian Computer Emergency Response Team
COTS	Commercial Off-The-Shelf
CS	Cybersecurity
CSF	Cybersecurity framework
DDoS	Distributed Denial of Service
DiD	Defense in Depth
EFIS	Estonian Foreign Intelligence Service
EU	European Union
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
ICS	Industrial Control System
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
KAPO	Estonian Internal Security Service
LFO	Load-follow Operation
MCDA	Multi Critera Decision Analysis
NIST	National Institute of Standards and Technology
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission
NEI	U.S. Nuclear Energi Institute
OT	Operational Technology
RIA	Information System Authority (Estonia)
SBOM	Software Bill of Materials
SCADA	Supervisory Control and Data Acquisition
SMR	Small Modular Reactor
SeBD	Security by Design
STUK	Radiation and Nuclear Safety Authority of Finland

Table of contents

List of figures

List of tables

1 Introduction

Estonia has initiated a plan to construct its first nuclear power plant, based on SMR technology, to address its growing energy needs and ensure dispatchable electricity generation. As the country has no prior experience with nuclear energy, it must develop a nuclear regulatory framework, including cybersecurity regulations adapted to the Estonian context and new challenges of modern NPPs, including SMRs.

Given the digital advancements and novel designs of SMRs, cybersecurity poses new risks compared to traditional nuclear facilities [1]. These risks are amplified by Estonia's regional security situation, characterized by increasing cyber and hybrid attacks against the state's critical infrastructure. Therefore, cybersecurity must be integrated as a fundamental part of Estonia's nuclear program from the earliest stages.

Past cyber incidents targeting the energy sector demonstrate why cybersecurity must be integrated from the early stages of the development lifecycle. In 2015 and 2016, Ukraine experienced coordinated cyberattacks against its power grid, which caused regional blackouts and disrupted grid operations through malicious control of SCADA systems [2]. These incidents showed that operational technology in the energy sector can be a deliberate and vulnerable target. A more recent example comes from India, where in 2019, Kudankulam NPP was targeted by a cyber-attack involving the Dtrack malware, attributed to the North Korean Lazarus Group. While the malware did not compromise critical control systems, it infiltrated administrative networks, raising concerns about potential future threats [3]. These examples show how digital vulnerabilities in complex control systems can be exploited to cause real-world damage, including public safety risks and geopolitical consequences.

While various international cybersecurity frameworks and standards exist, there is little publicly available research on how these standards apply to countries that are initiating their first nuclear programs. Estonia's case thus presents a unique opportunity to develop cybersecurity regulations tailored to national conditions and emerging threats.

This thesis aims to identify the most suitable cybersecurity standards, guidelines, and frameworks for Estonia's SMR project by analyzing international best practices and evaluating them through a multi-criteria lens, considering the Estonian context. It also presents recommendations based on expert interviews and literature analysis for implementing the selected standards and integrating nuclear cybersecurity best practices into the national SMR program.

1.1 Motivation

In 2019, the Estonian company Fermi Energia initiated planning and feasibility studies for the construction of an SMR nuclear power plant.[1] The initiative has since gained support at both the governmental and parliamentary levels,[2] driven by the country's need to secure affordable, stable, and low-carbon electricity generation for the future. Key motivators include an ongoing electricity deficit that forces Estonia to rely on imports, insufficient dispatchable generation capacity, and the imperative to meet climate neutrality goals by phasing out fossil fuel-based generation [4].

Nuclear energy, and specifically SMRs, are seen as a viable and complementary solution to Estonia's evolving energy mix. SMRs offer the potential for flexible, grid-stabilizing dispatchable generation while supporting decarbonization and national energy security goals [5]. Fermi Energia has conducted several studies on the environmental, economic, and technical feasibility of SMRs deployment in Estonia, laying the groundwork for further development.[3]

Despite these advancements, no public study has comprehensively addressed the cybersecurity implications of implementing an SMR in Estonia. Given the country's geopolitical position, recent years have seen a marked increase in hybrid threats, including cyberattacks and sabotage targeting critical infrastructure [6]. The cybersecurity of digitally advanced nuclear systems, such as SMRs, must be proactively addressed as a core component of Estonia's emerging nuclear regulatory framework. Recognizing this gap, and based on discussions with Fermi Energia, this thesis was

[1] https://majandus.postimees.ee/6553993/energiaettevote-tahab-eestisse-rajada-uue-polvkonna-tuumareaktorit
[2] https://www.err.ee/1609369496/riigikogu-otsustas-et-toetab-tuumaenergia-eestis-kasutuselevotmist
[3] https://fermi.ee/en/publikatsioonid/

initiated to examine cybersecurity considerations and recommend suitable frameworks and standards aligned with Estonia's specific conditions and needs.

1.2 Scope

This thesis focuses on the analysis and evaluation of cybersecurity frameworks and standards applicable to modern NPPs, with specific attention to Estonia's national context and prevailing cyber threat landscape. The study examines international cybersecurity frameworks, standards, and associated guidance and guidelines published by acknowledged organizations such as the International Atomic Energy Agency (IAEA)[1], International Electrotechnical Commission (IEC)[2], the National Institute of Standards and Technology (NIST)[3], and the International Organization for Standardization (ISO)[4]. These documents include strategic regulatory guidance, technical guides and standards, and implementation guidelines. For clarity, the term "frameworks and standards" is used throughout the thesis to refer to this broader group of normative documents.

It is important to note that cybersecurity frameworks and standards tailored explicitly for operational SMRs are currently limited, as only two SMRs are commercially operating globally, in China and Russia [7]. Therefore, the evaluation in this thesis draws upon publicly available and the latest cybersecurity frameworks developed for modern nuclear facilities, adapting them to the SMR context where appropriate.

Due to the classified nature of many technical and operational details related to nuclear systems, full access to proprietary or sensitive documentation was impossible. The analysis therefore relies exclusively on publicly available and freely accessible sources, including open standards, policy documents, academic literature, and expert interviews. Despite these limitations, the current level of transparency in Estonia's nuclear planning process, combined with stakeholder insights, provides a sufficient basis for meaningful analysis and evidence-based recommendations.

[1] https://www.iaea.org
[2] https://www.iec.ch/homepage
[3] https://www.nist.gov
[4] https://www.iso.org/

1.3 Research problem

Estonia is preparing to establish its first nuclear energy program and is required to develop a comprehensive regulatory framework from the ground up. Nuclear-specific cybersecurity regulations and guidelines must be an essential part of this framework. However, Estonia currently lacks experience in developing and implementing a nuclear legal framework, including nuclear-specific cybersecurity regulations. While several international and widely acknowledged CS regulations exist, they are not designed for direct implementation in countries starting their first nuclear programs [8]. Novel technologies and digital solutions of SMRs pose CS risks that challenge conventional regulatory models [1]. The absence of sufficient nuclear cybersecurity experience, combined with increasing regional cyber-threats to critical infrastructure, presents a significant challenge to the cybersecurity of Estonia's first planned SMR [6]. Therefore, there is a clear need to evaluate and adapt existing international cybersecurity frameworks and standards to Estonia's specific context.

1.4 Research questions

Based on the research problem and objectives described above, this thesis is guided by the following two main research questions with respective sub-questions:

Main Research Question (MRQ1)
How to identify the most suitable cybersecurity frameworks and standards to support the implementation of an SMR in Estonia?

To answer this question, the following sub-questions are addressed:

SRQ1: *What cybersecurity frameworks, standards, and guidelines are applied to SMRs and nuclear power plants in other countries?*
SRQ2: *How can these documents be evaluated and compared based on Estonia's national risk context and cybersecurity priorities?*

MRQ2: *What are the key cybersecurity challenges Estonia must address when preparing to implement an SMR?*

These questions are explored through a combination of qualitative expert interviews, literature review, and documentary analysis. Together, they support the development of a risk-informed and contextualized cybersecurity recommendation for Estonia's SMR initiative.

This master's thesis is divided into 9 chapters. The present and first chapter outlines the purpose and motivation of the thesis and presents the research questions. The second chapter provides a background context regarding the SMR implementation, national energy, cybersecurity challenges, and the study's theoretical background. The third chapter provides an overview of related work and existing literature in the field. In the fourth chapter, the author describes the research methodology and design, and approaches to data collection and analysis. The fifth chapter reflects the research findings and provides CS recommendations for the SMR program, as well as recommendations to the policymakers and regulatory authorities responsible for implementing nuclear CS oversight in Estonia. The sixth chapter provides an overview of the validation procedure and validates the research key outcomes. Chapter seven discusses the main findings and addresses questions that emerged during the validation process. Chapter eight outlines the study’s limitations and proposes directions for future work. Chapter nine reflects on the overall research process and its results and concludes with a summary and final remarks.

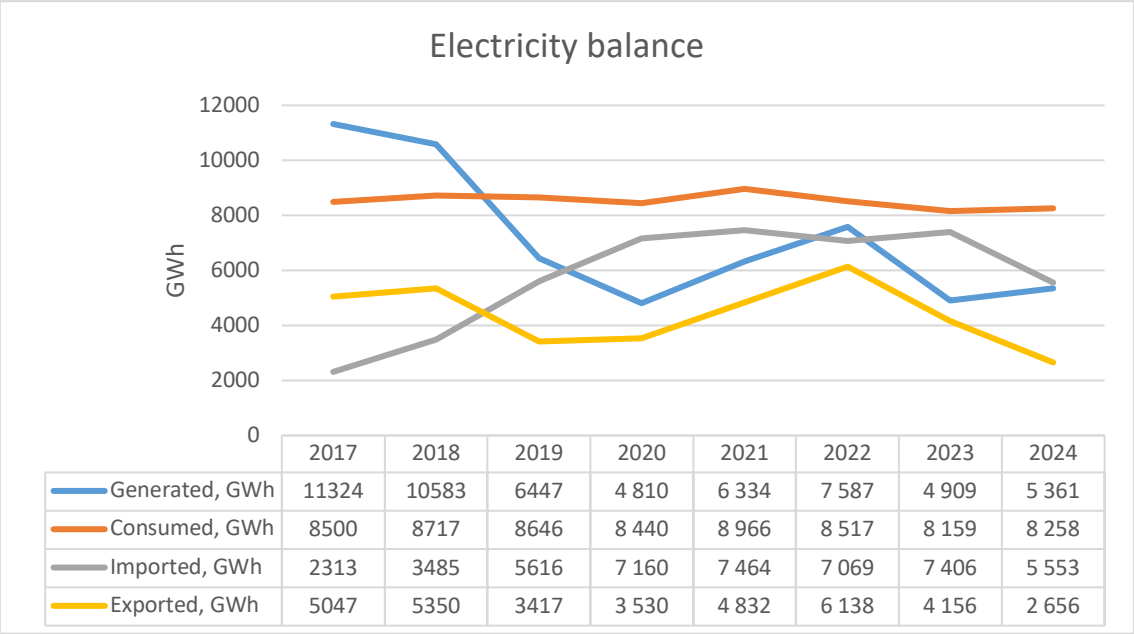
2 Background

This chapter provides the foundational background for the study, structured in two main parts: the practical context and the conceptual foundation. The first part explores Estonia's domestic energy policy challenges, the rationale for considering SMRs, the nuclear CS regulatory background, and the national cybersecurity threat landscape. These factors define the real-world problem space in which the research is situated. The second part outlines the conceptual basis for the evaluation method, including key considerations in cybersecurity governance, critical infrastructure risk, and regulatory suitability in newcomer nuclear contexts.

2.1 Practical background

Electricity generation in Estonia is largely based on renewable energy and legacy oil shale power plants. However, renewable sources are intermittent and non-dispatchable, while aging oil shale facilities are increasingly inefficient, costly, and environmentally unsustainable. As a result, dispatchable generation capacity has diminished sharply over the last decade. Due to insufficient market incentives and long-standing underinvestment, few new dispatchable generation facilities have been developed in Estonia [4].

The combined effect of declining domestic dispatchable generation capacity and growing reliance on electricity imports has created structural vulnerabilities in Estonia's energy system [4]. Notably, the country experienced significant electricity generation declines in 2019 following the decommissioning of oil shale units. Imports have since doubled to meet demand. This trend has contributed to sustained high electricity prices, increased exposure to regional market volatility, and diminished economic competitiveness. Figure 1 illustrates Estonia's electricity balance in the period 2017-2024, showing structural changes in energy generation and imports [9].



	2017	2018	2019	2020	2021	2022	2023	2024
Generated, GWh	11324	10583	6447	4 810	6 334	7 587	4 909	5 361
Consumed, GWh	8500	8717	8646	8 440	8 966	8 517	8 159	8 258
Imported, GWh	2313	3485	5616	7 160	7 464	7 069	7 406	5 553
Exported, GWh	5047	5350	3417	3 530	4 832	6 138	4 156	2 656

Figure 1. Electricity generation, consumption, import, export 2017-2024 .

The dramatic change in the geopolitical and security landscape in Europe following Russia's full-scale invasion of Ukraine in 2022 has also had a significant impact on the worsening of the situation. This has forced EU member states, including Estonia, to urgently reassess their energy security strategies as sanctions on Russian energy imports significantly disrupted the energy market and led to sharp increases in energy prices [10].

The resulting energy security deficit presents a strategic challenge for Estonia. The need for stable, low-carbon, and dispatchable power sources has grown more urgent amid the pressures of electrification, industrial growth, and the pursuit of climate neutrality goals. In this context, SMRs have emerged as a promising alternative. SMRs offer low-emission, grid-stabilizing power with a relatively small physical footprint and the potential for domestic deployment [5].

However, the adoption of SMRs introduces significant cybersecurity considerations, especially for a digitalized, high-threat environment like Estonia's. These risks are magnified by the absence of prior nuclear infrastructure or institutional experience in the country. A secure and context-sensitive regulatory foundation, including nuclear-specific cybersecurity, is therefore essential for Estonia's SMR development.

2.1.1 Small Modular Reactors (SMRs)

SMRs represent a new generation of nuclear reactors designed for modular construction, scalability, and enhanced safety. They are typically defined as reactors with an electrical output of up to 300 MWe per unit. Unlike conventional large-scale reactors, SMRs can be manufactured in centralized facilities, transported as modules, and deployed incrementally. This modularity enables faster deployment, cost predictability, and flexible integration into national energy systems [11]

SMRs are particularly suited to countries with small energy systems, limited grid flexibility, or the need for distributed, low-carbon energy solutions. They can be used for base load power, industrial or district heating, hydrogen production, or grid balancing in systems dominated by variable renewables. The majority of SMR designs incorporate passive safety features, reduced reliance on active cooling, and inherent fault-tolerant behavior, making them attractive from both safety and operational perspectives [5]

The SMR initiative is currently led by Fermi Energia, which has conducted preliminary feasibility studies and design evaluations. As a technical solution, the company has selected the BWRX-300 reactor design developed by GE Hitachi. This reactor is a Generation III+ boiling water reactor with a projected electrical output of 300 MWe and passive safety systems based on natural light-water circulation and gravity [12]. The BWRX-300 has already been submitted for design review in several countries, including Canada, the United States, and Poland. It is important to emphasize that the Canadian nuclear regulator (CNSC) has already approved the licensing of the BWRX-300, and construction is currently underway at the Darlington Nuclear Power Plant site[1].

While SMRs offer technical and economic advantages, they also may introduce specific cybersecurity challenges. The high degree of digitalization, remote diagnostics, integrated Instrumentation and Control (I&C) systems, and automated operation increase the complexity of cybersecurity planning. These systems often rely on commercial off-the-shelf (COTS) components, which may not meet nuclear-grade security standards.

[1] https://www.world-nuclear-news.org/articles/canadian-regulator-issues-smr-construction-licence

Moreover, the smaller organizational footprint of SMRs may reduce redundancy in cybersecurity roles and oversight [1],[13].

For Estonia, these challenges are compounded by the absence of a legacy nuclear industry, a dedicated nuclear regulatory authority, or operational experience in nuclear-grade cybersecurity [5]. Consequently, the adoption of international cybersecurity frameworks, adapted to the Estonian context and realities, is essential. The following sections address the regulatory environment and cyber-threat landscape shaping Estonia's preparedness.

2.1.2 Regulative background

Introducing nuclear energy in Estonia requires comprehensive legislative, institutional, and procedural preparation. This includes the development of a national regulatory framework for nuclear safety, radiation protection, licensing, and cybersecurity. Establishing these legal and technical structures is a prerequisite for implementing any nuclear project by a newcomer country [5].

Cybersecurity regulation poses a particularly complex challenge. According to the literature, even countries with a long-standing nuclear experience face difficulties in assessing SMR-specific cyber risks due to the novelty of the technology and lack of practical implementations [14], [15] Most SMRs are still in the licensing or pre-licensing phase, and only two SMRs are currently in commercial operation globally [7]. As a result, limited empirical data exists regarding the cybersecurity performance of SMRs.

In Estonia, the development of a cybersecurity framework for the planned SMR is expected to be guided by international best practices and aligned with the country’s legal and institutional structures [5]. Such a framework is expected to ensure comprehensive regulatory coverage across all phases of the reactor lifecycle, including planning, design, operation, and decommissioning.

In the reviewed literature and documentation, a core set of organizations issuing cybersecurity standards and regulatory guidance relevant to nuclear and industrial control systems is identifiable. The most recognized among these are the International Atomic Energy Agency (IAEA), International Electrotechnical Commission (IEC), International

Organization for Standardization (ISO), U.S. National Institute of Standards and Technology (NIST), and U.S. Nuclear Regulatory Commission (NRC).[1]

In the EU context, regulatory requirements also arise from the NIS2 directive (Directive (EU) 2022/2555) and the Critical Entities Resilience (CER) directive, both of which establish baseline cybersecurity and resilience obligations for essential service operators, including the energy sector. However, these directives are not nuclear-specific and must be supplemented by sectoral regulation [16], [17].

As Estonia designs its regulatory approach, the experience of nearby Finland offers a valuable reference. Finland's nuclear regulator, STUK,[2] has developed detailed cybersecurity guidelines as part of its broader security framework. These documents represent very mature national-level approaches to nuclear cybersecurity and align well with Estonia's institutional proximity, energy security concerns, and SMR ambitions [18]. As such, Finnish practices and standards are highly relevant for Estonia as a peer reference case.

In summary, Estonia must proactively identify, evaluate, and adapt international cybersecurity frameworks to form the foundation of its own nuclear regulatory system. This includes selecting baseline standards and establishing implementation strategies that reflect Estonia's specific risk environment, technical capacity, and SMR deployment path. The following section presents the regional cyber threat landscape that further contextualizes this regulatory need.

2.1.3 Energy sector's cyber-threat situation in the region

Energy sector, as an important part of national security and economic resilience, faces an increasingly complex and hostile cyber-threat landscape. Despite Estonia's high level of digital maturity and acknowledged cybersecurity capacity, the evolving geopolitical environment, particularly in light of the ongoing war in Ukraine, has intensified hybrid threats across all critical infrastructure sectors [6], [19]

[1] https://www.nrc.gov/about-nrc.html
[2] https://stuk.fi/en/frontpage

The Estonian Information System Authority (RIA) reports a growing number of targeted cyber incidents, including ransomware, phishing, and more sophisticated intrusions against energy sector entities. According to its 2024 and 2025 assessments, the number of critical infrastructure-related cyberattacks has steadily increased, with evidence of persistent reconnaissance activity and capability development by hostile actors[6], [20].

RIA's CERT-EE and Estonian Internal Security Service (KAPO) have identified the energy sector as among the most exposed due to its high degree of digitalization, remote controllability, and cross-border market integration [6], [21]. Transmission networks, balancing systems, and vendor-managed control interfaces present a range of attack vectors. Estonia's participation in the Nord Pool market and its interconnection with regional grids introduce additional complexity and threat exposure [19].

State-aligned cyber operations are assessed by the Estonian Foreign Intelligence Service (EFIS) as strategically motivated. They are designed not merely to cause disruption, but to test national resilience and influence political decision-making. EFIS has explicitly linked Russian military intelligence units to attempts to destabilize critical infrastructure, including energy systems [19], [22].

Additional risks arise from supply chain dependencies. EFIS warns that technologies and equipment sourced from authoritarian regimes, including Chinese-manufactured components, may be subject to foreign intelligence influence. This risk is particularly acute in sectors where technical surveillance and maintenance are vendor-dependent [22].

RIA's cybersecurity maturity assessments show that while energy sector operators have adopted basic cybersecurity controls (e.g., segmentation, logging, intrusion detection), systemic gaps persist. These include limitations in incident response readiness, third-party risk management, and the ability to coordinate across sectors and ministries [6], [23].

As Estonia proceeds toward the introduction of SMRs, these cyber threat dynamics take on a heightened significance. SMRs rely on advanced digital I&C systems and may involve extensive vendor integration. Without an existing nuclear cybersecurity regulatory foundation or institutional experience, Estonia faces a compounded risk. These conditions demand a tailored and proactive approach to cybersecurity governance in the nuclear domain.

2.2 Theoretical foundation

This study is primarily grounded in a risk-informed and context-aware evaluation approach to assess the suitability of cybersecurity frameworks and standards for Estonia's first SMR program. Throughout the thesis, this is referred to as a risk-contextual approach. In critical infrastructure sectors, especially nuclear energy, cybersecurity regulations must be adapted to the national security environment, cyber-threat landscape, institutional maturity, and sector-specific requirements. This approach is supported in the literature, which emphasizes that cybersecurity frameworks and standards are not universally applicable but must be aligned with the operational, legal, and geopolitical context in which they are implemented [24], [25]

Estonia's position as a nuclear newcomer in a high-threat region presents unique cybersecurity governance challenges. Standards designed for established nuclear states may not fully address the risks Estonia faces. Therefore, this study evaluates frameworks based on criteria reflecting Estonia's regulatory gaps, digital dependency, and evolving threat profile. These criteria were derived from national CS threat reports, expert interviews, and thematic literature analysis [6], [19], [22].

The document evaluation process used a structured, criteria-based scoring method, inspired by comparative evaluation logic but not following any formal MCDA[1] techniques. Each document was assessed on a simple 1–5 scale across predefined criteria, allowing for transparent, qualitative comparison. This method is especially suited to exploratory case study research, where flexibility and contextual relevance are more important than mathematical precision.

Some previous works applied detailed subcategory mappings to benchmark coverage against frameworks like NIST CSF [26]. While appropriate for mature regulatory environments, such methods may not fit the early-stage regulatory planning of nuclear newcomer countries. This study instead prioritizes context-specificity, institutional fit, governance readiness, and adaptability.

[1] https://analysisfunction.civilservice.gov.uk/policy-store/an-introductory-guide-to-mcda/

3 Related work

This chapter provides a review of relevant literature to contextualize the research problem and establish a foundation for evaluating cybersecurity frameworks and standards for SMRs in Estonia. The review does not follow a systematic literature review (SLR) protocol but applies a focused narrative approach aimed at identifying key academic and institutional contributions in the intersecting domains of SMR development and cybersecurity [27].

The objective is to assess the distinctive technical, operational, and regulatory characteristics of SMRs compared to conventional nuclear power plants, thus identifying cybersecurity challenges specific to SMRs. This enables the author to synthesize existing evaluations and proposals for cybersecurity frameworks applicable to nuclear energy systems, particularly those relevant to states with emerging nuclear programs.

Special attention is given to works published in the last five years, reflecting the increasing academic and regulatory interest in SMR's cybersecurity since 2019. Although the number of academic studies remains limited, especially for newcomer nuclear nations like Estonia, the reviewed literature helps identify critical concerns and guide the selection of relevant frameworks evaluated in this thesis.

The following sections examine the advantages of SMRs and the cybersecurity risks inherent in their digitalized architecture; discuss broader implementation challenges, including gaps in regulatory readiness and institutional capacity; and outline the current landscape of cybersecurity frameworks and standards proposed for nuclear or industrial control system contexts.

3.1 Advantages and cybersecurity challenges of SMRs

SMRs represent an emerging class of nuclear energy technology designed for modular construction, enhanced safety, and flexible deployment. Compared to traditional nuclear power plants with outputs of over 1000 MWe, SMRs typically produce up to 300 MWe and are intended to be manufactured off-site and transported as prefabricated units. Their

compact size and scalable deployment offer several advantages for countries with smaller energy systems or limited infrastructure [11], [28].

The literature highlights a range of technological and operational benefits associated with SMRs. These include reduced land use due to smaller site requirements, cost-efficiency through modular construction, and improved safety via passive safety features and fault-tolerant reactor designs [5]. Moreover, SMRs are capable of autonomous and remote operations, which allows for reduced staffing and operational costs, and load-follow operation (LFO), enabling dynamic adjustment of output to grid demand [29]. These characteristics make SMRs attractive for grid balancing, industrial applications, and integration into low-carbon national energy strategies [29].

However, these advantages introduce unique cybersecurity challenges. Unlike traditional reactors that rely largely on analog systems, SMRs are built around advanced digital I&C systems, often incorporating COTS components and networked architectures. This digitalization exposes SMRs to a broader array of cyber threats [1], [30] .

Several researchers have raised specific concerns. Aamoth (2020) emphasizes that remote operation and digital management, while economically beneficial, increase the attack surface by replacing human supervision with software-driven processes [1]. Similarly, Ayodeji and Ahmed (2021) offer a detailed taxonomy of cyberattack propagation paths in nuclear digital systems, highlighting vectors such as programmable logic controllers, actuator signals, human factors, and supply chain dependencies [13]. These latter two risks are particularly acute for SMRs due to their modular assembly from off-site, vendor-controlled components, often sourced internationally [30].

In the Estonian context, these cybersecurity issues are intensified by the absence of domestic nuclear experience and the challenge of building nuclear cybersecurity capabilities from the ground up [5]. Additionally, insider threats and supply chain integrity, particularly from potentially untrusted vendors in third countries, necessitate increased scrutiny in SMR deployments [13]. Overall, while SMRs offer substantial opportunities for secure, clean, and decentralized energy production, they also introduce new and underexplored cybersecurity risks. Addressing these requires careful regulatory adaptation, particularly for newcomer states like Estonia.

3.2 Cybersecurity integration in SMR design and engineering

Several recent studies emphasize that cybersecurity for SMRs must be closely aligned with each reactor's specific technical characteristics [31]. R. Fasano stresses the importance of recognizing that different types or designs of advanced reactor concepts possess unique I&C system architectures, which require tailored security approaches. Consequently, it is not feasible to mitigate cybersecurity risks for SMRs through a unified or overly standardized framework [31]. Each SMR design must be assessed individually, based on its architectural and functional context. As Fasano concludes: “Identifying cyber vulnerabilities in the diverse and complex systems architectures in the design phase is critical to ensure that these vulnerabilities are minimized in the operation phase [31].”

In response to these challenges, R. Duguay of the Canadian Nuclear Safety Commission proposes the integration of security by design (SeBD) principles into regulatory frameworks. This approach advocates for embedding cybersecurity considerations into the earliest design stages, enabling more flexible and effective mitigation of digital threats while ensuring alignment between safety and security objectives. SeBD, as a lifecycle concept, supports a continuous security posture across design, deployment, and operation [32].

Further elaborating on this principle, researchers at Idaho National Laboratory (INL) argue that even SeBD may not sufficiently account for the full spectrum of cyber risks. According to INL, digital I&C systems must address both adversarial threats, like malicious actors, and unintentional risks (e.g., software flaws, misconfigurations) from internal and external sources. To overcome the limitations of compartmentalized cybersecurity strategies, INL proposes a holistic engineering approach in which cybersecurity is not treated as an isolated domain. Instead, it is embedded as a co-equal design input alongside safety, reliability, functionality, and performance objectives. Such integration ensures that cyber risk management is structurally inseparable from the broader engineering lifecycle [33].

3.3 Cybersecurity frameworks for the nuclear sector

Several cybersecurity frameworks have been developed over the past two decades to address the growing complexity of industrial control systems (ICS) and critical infrastructure protection [34], [35]. In the nuclear domain, however, the application of these frameworks must contend with domain-specific requirements such as safety-security integration, supply chain integrity, and long asset lifecycles. For Estonia, selecting or adapting an appropriate set of cybersecurity standards demands critical consideration of both international best practices and the contextual needs of a newcomer nuclear state [5].

The International Atomic Energy Agency (IAEA) has published several Nuclear Security Series (NSS) documents, such as NSS 17-T, NSS 42-G and NSS 33-T, which provide well-defined guidance on implementing cybersecurity for nuclear facilities [24], [36], [37]. These are complemented by sector-specific standards like IEC 62645, which offers a structured framework for managing cybersecurity in nuclear I&C systems, and IEC 62859, which addresses interface dependencies between safety and security [38], [39]. However, in his survey, J. Linnosmaa (2021) notes that there remain significant implementation gaps, particularly where guidance is either too general or fails to account for emerging digital dependencies in newer reactor designs such as SMRs [40].

This gap becomes even more critical in light of challenges specific to SMRs. C. Siserman-Gray (2023) emphasizes that SMRs introduce new regulatory blind spots due to their modular design, remote operation capability, and the off-site involvement of multiple vendors. Many SMR projects begin cybersecurity-relevant decisions in the vendor phase, prior to licensing, creating a mismatch with conventional regulatory triggers. The authors argue that frameworks like NRC 10 CFR 73.54 or NEI 08-09 are insufficient without early-phase engagement, vendor oversight mechanisms, and integration of cybersecurity by design [41].

The Arinze (2023) study from the Nigerian Nuclear Regulatory Authority reinforces this view from a newcomer perspective. The paper highlights the difficulty of applying generic national cybersecurity strategies to nuclear environments without domain-specific regulations and institutional coordination. It calls for integrating cybersecurity into the full lifecycle of nuclear oversight, and for regulators to avoid over-relying on ICT

ministries or cybersecurity centers outside the nuclear domain [8]. For Estonia, which currently lacks institutional capacity in nuclear-specific cybersecurity, this insight supports the need to develop embedded regulatory structures early in the SMR program.

An early academic contribution to the comparison of nuclear cybersecurity standards was made by Eve Hunter in her 2016 master's thesis at TalTech. Her work examined nine cybersecurity documents relevant to nuclear facilities, using the NIST Cybersecurity Framework 2014 as a reference model. The study applied a matrix-based method to statistically map the coverage of CSF subcategories across the selected documents, treating controls in a largely mechanical and quantitative manner. One of the key findings was that no single document could be considered sufficient for implementation on its own, and that a hybrid approach by combining multiple complementary sources is necessary. The research, however, leaned toward a U.S.-centric perspective, both in document selection (including NEI 08-09, NIST SP 800-53, and NERC CIP) and in the geographic background of the consulted experts [26].

Lastly, Choi (2023) provides a technical risk forecast tailored specifically for SMRs. They identify four advanced SMR features, such as autonomous operation, remote control, load-following integration, and modular supply chains, as high-risk areas inadequately addressed by legacy standards. Their findings recommend the integration of frameworks like IEC 62443 (network segmentation), ISO/IEC 27036 (supply chain security), and SBOM-based transparency tools, especially given the growing use of COTS and third-party software in reactor designs. These insights directly validate the risk-contextual evaluation approach used in this thesis, which incorporates criteria for governance scalability, supply chain assurance, and EU compatibility [29], [30].

3.4 Key insights and identified research gaps

The reviewed literature demonstrates that while numerous cybersecurity standards exist, none fully address the combined needs of digitalized, vendor-dependent, and highly networked SMRs. Developing an initial nuclear cybersecurity framework requires not only a careful selection of internationally recognized norms but also national-level adaptation based on contextual threats, institutional readiness, and lifecycle governance.

The reviewed literature demonstrates a growing international interest in SMR cybersecurity, with the majority of relevant academic contributions emerging since 2019. This trend reflects both the accelerating development of SMR technologies and a widening recognition of the cybersecurity challenges they present. Several studies have offered valuable frameworks, risk taxonomies, and conceptual models for integrating cybersecurity into nuclear design and regulation. However, these remain largely theoretical, and practical implementation strategies are still underdeveloped, especially for countries in the early stages of establishing their nuclear infrastructure.

Importantly, existing case studies and technical analyses often focus on countries with long-standing nuclear programs, such as Canada, the U.S., and South Korea [30], [32], [41]. While these provide valuable reference points, they do not fully account for the institutional, legal, and technical challenges faced by nuclear newcomer countries [8]. Moreover, publicly available research offers limited insights into the cybersecurity readiness or regulatory adaptation required for specific SMR designs, including the BWRX-300 selected for deployment in Estonia [12].

The literature further highlights that SMRs are not technologically unified. Their I&C system architectures, operational models, and integration pathways differ significantly by design. Consequently, cybersecurity assessments must be tailored rather than standardized [31]. Several authors emphasize the importance of Security by Design and lifecycle-based approaches, yet detailed methodologies for newcomer states remain largely unexplored [32], [33]. Additionally, due to the limited number of SMRs in commercial operation, most threat detection strategies rely on simulations or theoretical modeling using virtual testbeds or digital twins [42].

In conclusion, while the academic discourse around SMR cybersecurity is expanding, significant research gaps persist. There are no comprehensive public studies addressing the cybersecurity regulatory requirements for SMRs in newcomer nuclear states. Nor are there detailed assessments of the cybersecurity implications of planned BWRX-300 SMR deployment in Estonia [12]. This thesis aims to address these gaps by evaluating applicable cybersecurity standards through a context-informed lens and offering recommendations tailored to Estonia's specific institutional and national security context.

4 Research design and methodology

Due to the multi-layer and complex nature of the research problem, the research follows the exploratory case study research methodology, enabling an in-depth understanding of SMR CS requirements and needs in the Estonian context [43], [44]. The chosen methodology allows for understanding the research problem from different perspectives and a better understanding of this complex phenomenon. An exploratory case study is well-suited and facilitates the understanding of the nature of the research problem, as, at this stage, the level of uncertainty in the SMR implementation in Estonia is high [43], [44].

The research was divided into three main stages, starting from the problem definition and case selection to the validation and final conclusions. Figure 2 presents the concrete research steps following the case study research process.

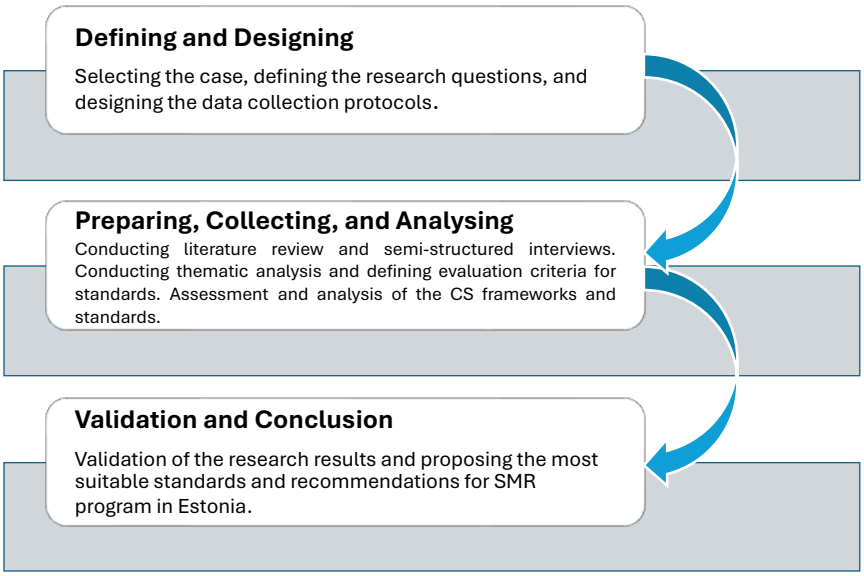


Figure 2. General overview of the research design.

As previously emphasized in section 2.2, the risk-contextual approach was used to identify evaluation criteria, ensuring that the evaluation and prioritization of widely referenced cybersecurity frameworks and standards were grounded in Estonia's specific CS threat landscape, cyber-risks, and national context [5], [6], [19], [22]. Also, data collected via expert interviews was explicitly considered when evaluating cybersecurity standards.

4.1 Data collection and analysis

Three primary data sources were used in the study: expert interviews, literature review, and secondary data sources. Semi-structured expert interviews were conducted with key representatives from Fermi Energia, Eesti Energia, RIA, and relevant government agencies. A literature review focused on peer-reviewed publications addressing SMR cybersecurity challenges and governance. In addition, secondary data sources included cybersecurity and technical reports, institutional and government documents, legal acts, whitepapers, guidelines, and standards.

Table 1 summarises the relationship between these data sources and the research questions, indicating which sources contributed to addressing each specific question.

Table 1. Data sources to research questions mapping.

Research question	Expert interviews	Literature review	Secondary data sources
MRQ1	X	X	X
SRQ1		X	X
SRQ2	X		X
MRQ2	X		X

A thematic analysis was used to extract the most important cybersecurity challenges, regulatory needs, and risk perceptions from expert interviews, policy documents, and relevant academic literature [45]. This method enables systematic identification of patterns across diverse qualitative inputs. The resulting themes served as the basis for constructing the risk-contextual criteria used later in the evaluation and scoring process of selected CS frameworks and standards.

The analysis consisted of two parallel streams – the analysis of expert interview data and the analysis of regulatory documents. These streams were based on distinct data sources. Thematic analysis was conducted across interview transcripts and national CS threat reports to extract the main cybersecurity priorities relevant to Estonia's national context. These themes were used to define evaluation criteria that reflect the practical and strategic cybersecurity needs for SMR implementation. In parallel, academic literature and secondary data sources provided information on the most referenced CS frameworks, standards, and guidelines in the nuclear domain, enabling the creation of an initial list of potentially relevant CS frameworks and standards for the study context. The selected

frameworks and standards were evaluated against criteria derived from identified themes of the interview data. Thematic summaries of the interview's data and CS documents evaluation results were synthesized and interpreted, forming the results and outcomes of the study, which were validated through expert interviews. The detailed analysis process is visualized in the following Figure 3.

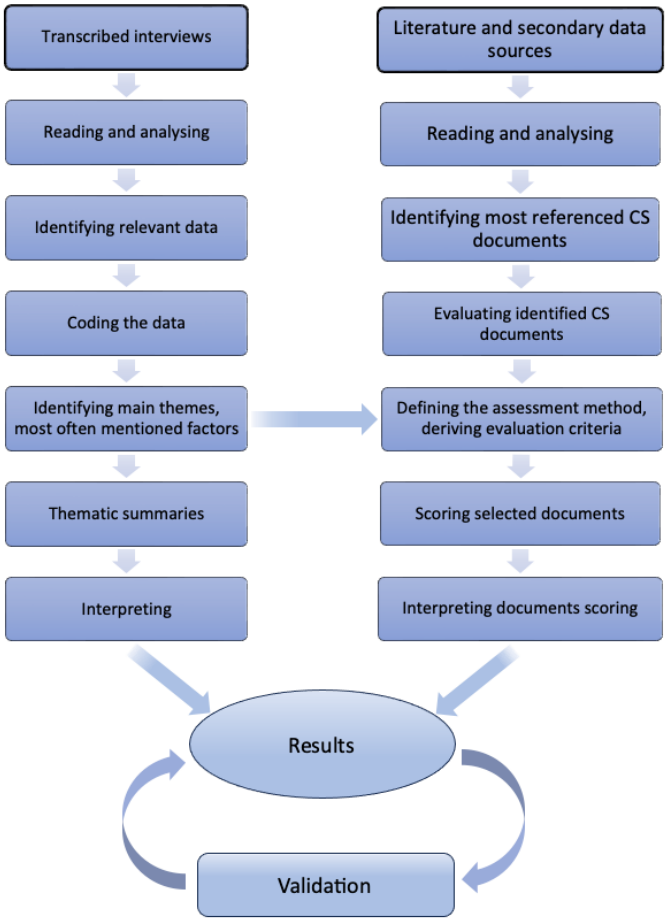


Figure 3. Data analysis model.

4.2 Context-aware evaluation approach

The evaluation process used in this thesis is grounded in a risk-informed and context-aware approach, which was defined by the author as the risk-contextual approach. It emphasizes evaluating cybersecurity frameworks and standards in relation to the country's specific threat environment, identified risks, institutional maturity, and legal conditions as a nuclear newcomer. This approach is not based on a standardized and formally defined method but conceptually draws from the principles of context-aware risk management outlined in ISO/IEC 27005 and risk-informed security program

development in IAEA NSS 17-T. Both normatives recommend tailoring security measures to the specific risks and contextual realities faced by an organization or national regulatory body [24], [25].

In this study, the risk-contextual approach was applied by identifying country-specific challenges through expert interviews, national cyber-threat assessments, and comparative regulatory analysis. These included, among others, the absence of a dedicated nuclear regulatory framework, legal constraints around vendor exclusion, and the cyber-threat landscape in the country. From this, six evaluation criteria were derived to reflect the most acute cybersecurity dimensions relevant to the first SMR implementation effort.

The use of a risk-informed and context-aware approach is particularly justified in this study, given the absence of legacy nuclear cybersecurity regulation in Estonia and the need to design an initial governance foundation from the ground up. Rather than benchmarking technical features or control coverage, this approach allows for assessing the strategic and institutional suitability of each framework for adoption in the Estonian SMR context. This method allows for a flexible, qualitative, and expert-informed evaluation process tailored to an exploratory national case study, while remaining aligned with international cybersecurity governance principles.

4.3 Validation approach

To ensure the credibility and practical relevance of the research findings, a validation process was conducted using methodological triangulation [46]. This included cross-verification from three primary data sources: peer-reviewed literature, expert interviews, and secondary data sources.

In addition, follow-up interviews were held with domain experts from Fermi Energia, RIA, and the Ministry of Interior. These experts reviewed the evaluation criteria, scoring rationale, and preliminary rankings of the cybersecurity frameworks and standards, as well as proposed recommendations with justifications. Based on their feedback, corrections and adjustments were made to the final results interpretation and recommendations. This validation approach strengthens the reliability of the thesis recommendations, particularly in the absence of operational nuclear infrastructure in Estonia.

5 Results

This chapter presents the primary outcomes of the study by outlining the results and recommendations extracted from the analyzed dataset. It is organized into four sections: the analysis and results of expert interviews; the evaluation of selected CS frameworks and standards; and recommendations based on the results.

5.1 Interview results and analysis

To address the second main research question (MRQ2) and to support answering MRQ1, the author conducted five semi-structured expert interviews between March 4 and April 11, 2025. Interviewees were selected based on their expertise and institutional relevance to nuclear energy, cybersecurity in the energy sector, or policy shaping in Estonia. Given Estonia's limited experience in the nuclear domain, this small sample represents a significant portion of the country's available expert pool in the field of nuclear cybersecurity.

The interviews were conducted in Estonian and recorded with the interviewees' prior consent. Interview durations ranged from 36 to 95 minutes. A semi-structured approach was adopted: a core set of questions was prepared (see Appendix 2), but the interviewer adjusted the flow and content based on the interviewee's area of specialization. This format allowed for spontaneous follow-up questions and deeper exploration of context-specific issues. The questionnaire was thematically aligned with the main research questions, particularly regarding Estonia's cybersecurity readiness, regulatory environment, and framework selection for SMRs.

An overview of interviewee roles, institutional affiliations, and sectoral responsibilities is presented in Table 2. The selection was made using a snowballing strategy, where each interviewee was asked to recommend further relevant experts. This method proved valuable in identifying knowledgeable individuals, including some not originally targeted, such as a Member of Parliament, whose perspective introduced political and strategic insight into Estonia's nuclear ambitions.

Table 2. List of interviewed experts.

Organization	Role in SMR process	Job position	Sectoral expertise
Fermi Energia	SMR's licensee; operator	Chief Technology Officer	Nuclear energy and power plants
Eesti Energia	Energy sector's CS expertise, advisory in CS matters	Chief Information Security Officer	Information and cybersecurity in the field of critical infrastructure and energy
RIA	Critical infrastructure CS expertise, advisory in CS matters	Cybersecurity Centre of Critical Infrastructure, head of tech. department	Critical infrastructure and vital services cybersecurity
Minsitry of Interior	Nuclear security expertise, nuclear policy development	Nuclear Security and Emergency Preparedness advisor	Nuclear security, safety and safeguards; nuclear regulations
Parliament of Estonia	Nuclear policy, legislation environment	Member of Parliament, Member of the Economic Affairs Committee	Experimental particle physics, energy policy in parliament, SMR topics

While most interviewees had no direct experience with cybersecurity in nuclear environments, several had participated in or advised on the digital security of energy systems such as wind farms, battery storage, and solar plants. Their insights highlighted current practices, limitations, and potential parallels with SMR implementation. From the interviews, several key themes and patterns emerged:

Procurement and Supply Chain Risks: Experts voiced concern that the state procurement law currently does not allow exclusion of vendors based on national origin, limiting the ability to mitigate geopolitical risks in supply chains. Several interviewees emphasized the importance of full control over I&C system origin and advocated for vendor trust verification and background screening.

Security-by-Design, Cybersecurity-by-design, and Project Integration: Multiple participants noted that cybersecurity has historically been integrated too late in the infrastructure lifecycle. In the case of SMRs, they stressed the need to embed security requirements at the design stage, rather than retrofitting controls post-procurement. The concept of security by design and cybersecurity by design was referenced as essential but underused in Estonian energy infrastructure projects.

Regulatory Uncertainty: The absence of a designated authority or structured roadmap for nuclear cybersecurity governance in Estonia was raised as a serious gap. Interviewees disagreed on whether the Ministry of Climate, RIA, or a future nuclear regulatory body should lead the effort.

Institutional and Human Resource Constraints: Participants acknowledged the limited national talent pool in both nuclear and cybersecurity fields, warning that long-term capacity building must begin early to ensure SMR oversight readiness. Estonia's strong IT sector was noted as an asset, but insufficient alone for nuclear cybersecurity needs.

Cyber Threat Landscape and Insider Risk: All interviewees agreed that during the execution of the SMR program in Estonia, hybrid threats would likely increase. These might include misinformation campaigns, insider manipulation, and remote cyberattacks. They cited examples of past influence operations in the Baltic region and stressed the importance of resilience planning against insider threats and advanced persistent threat (APT)[1] activity.

Political Momentum and International Support: Interviewees noted that Estonia is having high public and political support for nuclear energy, and has already secured strong collaboration with IAEA, Euratom[2], and advisors from countries like Finland, Canada, and the U.S. This was seen as a positive enabler of best practice adoption, though participants cautioned that local adaptation will still be required.

In summary, the interviews highlighted several urgent technical, institutional, and legislative gaps that must be addressed before Estonia proceeds with SMR deployment. These insights directly informed the development of the risk-contextual criteria used for evaluating cybersecurity frameworks and standards in section 5.2.

[1] https://csrc.nist.gov/glossary/term/advanced_persistent_threat
[2] https://euratom-supply.ec.europa.eu/index_en

5.1.1 Strategic readiness analysis: expert-informed SWOT

Based on the data collected through expert interviews, the author aimed to examine Estonia's current capabilities and readiness for the implementation of an SMR and the broader nuclear energy program. Particular attention was given to the Estonian energy sector and the role of cybersecurity in managing nuclear facilities. To conduct this assessment, the author employed the SWOT analysis methodology, evaluating both internal conditions (strengths and weaknesses) and external factors (opportunities and threats) that may influence the future development of the sector [47]. The findings are summarized in the visual representation provided in Figure 4.

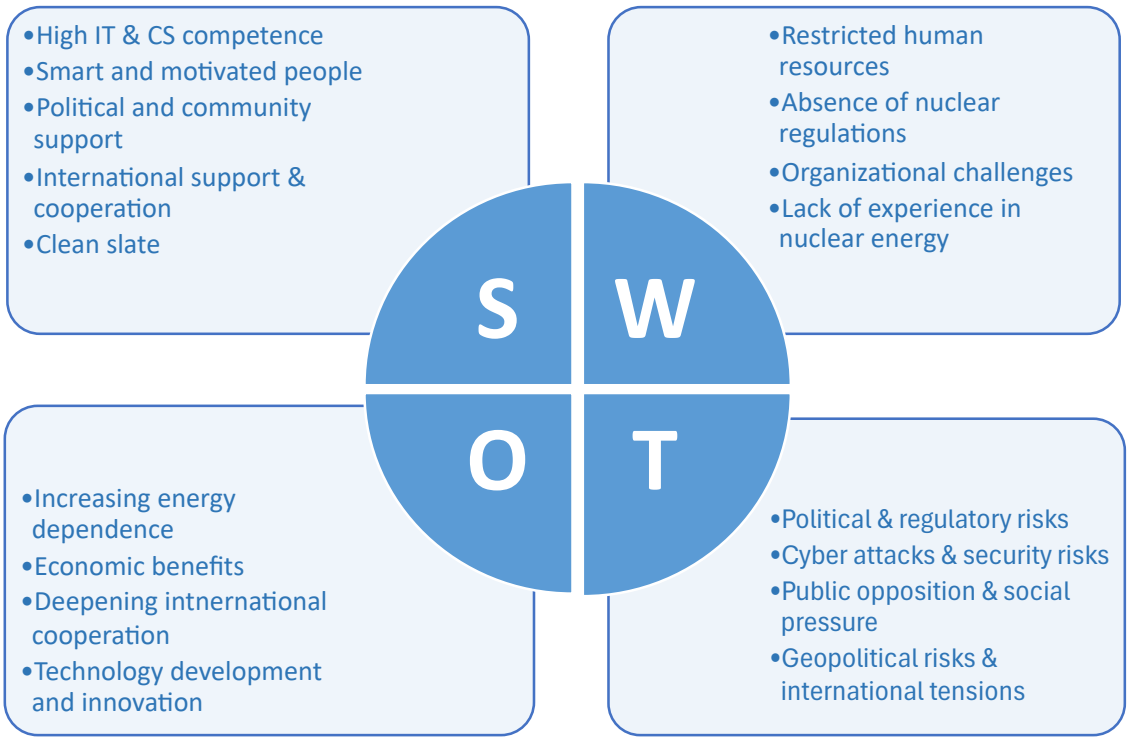


Figure 4. SWOT Analysis of Estonia's readiness for nuclear program implementation.

The summarising graphical representation was developed based on a detailed analysis of the interview data collected by the author. The following summary outlines the main findings of that analysis.

Based on expert input, the author identifies several strengths that support the feasibility of establishing an SMR in Estonia:

1) Estonia is internationally recognised for its strong IT sector and cybersecurity expertise, which exceeds the global average and provides a solid foundation for secure digital infrastructure.
2) The population is generally well-educated and motivated, which contributes to favourable conditions for launching and sustaining complex technological initiatives.
3) Political and societal support for nuclear energy is strong, with endorsement from the government, parliament, and general public.
4) Estonia benefits from international cooperation and support, including technical and strategic assistance from organisations such as the IAEA and Euratom, and collaboration with experts from the USA, Finland, and Canada.
5) The absence of legacy nuclear infrastructure enables Estonia to apply modern best practices and avoid past mistakes made by more established nuclear nations.

In parallel, the analysis also revealed several structural and institutional weaknesses that could pose challenges to SMR deployment:

1) Due to Estonia's small population, the availability of qualified specialists is limited, which may affect the long-term sustainability of national nuclear oversight and operations.
2) There is currently no established legal framework for nuclear energy, which may delay or complicate the implementation of the SMR project and broader regulatory development.
3) The creation of a new regulatory body or specialised organisational structures will be necessary to ensure effective oversight and safe management of nuclear technologies.
4) Although Estonia demonstrates strong general cybersecurity and technical competence, there is a significant lack of domain-specific nuclear cybersecurity experience, which will need to be addressed through targeted capacity-building.

The analysis also identified several forward-looking opportunities and potential external threats that may significantly influence the success or failure of Estonia's nuclear energy initiative. Identified opportunities were as follows:

1) The deployment of nuclear energy could significantly reduce Estonia's dependence on imported energy, thereby enhancing national energy security and resilience.

2) The construction and operation of SMRs present opportunities for economic revitalisation, including the creation of high-value jobs, the development of supporting infrastructure, and long-term reduction in electricity costs.
3) Estonia will be able to deepen its engagement with the international nuclear community, benefiting from cooperation with expert organisations and the ability to implement proven best practices.
4) Adoption of SMR technology creates a platform for introducing the latest innovations, including new generation safety systems and digitally integrated plant management solutions.

Identified threats:

1) Domestic political shifts or regulatory delays may disrupt or halt nuclear program development, posing risks to the continuity of the SMR initiative.
2) Nuclear facilities are attractive targets for cyberattacks, which could endanger operational safety, critical systems, and national confidence in the technology.
3) Public opposition or community-level resistance, especially when amplified by disinformation campaigns, could undermine political support and delay licensing or site approval processes.
4) Geopolitical instability and hybrid threats from hostile states could increase both physical and cyber risks, making national coordination and resilience planning essential to program viability.

From the data collected during the interviews, mainly from the transcribed texts of the interviews, the analysis enabled the filtering and synthesis of key opinions, perspectives, and recurring themes. This informed the identification of strengths, weaknesses, opportunities, and threats in the context of Estonia's planned SMR deployment. Paradoxically, the lack of prior experience in the field of nuclear energy emerged as both a weakness and a strength. On one hand, it represents a significant challenge, requiring extensive effort to build regulatory, institutional, and technical competence from the ground up. On the other hand, it presents a unique opportunity to establish a nuclear program without legacy constraints, applying latest best practices and drawing upon broad international support to design an efficient and secure framework from inception.

5.2 CS frameworks and standards evaluation

This section presents the assessment results of CS frameworks and standards, detailing the selection process, the development of assessment criteria, the use of these criteria in scoring, and the interpretation of the assessment findings. Although some subsections describe preparatory steps and methodological details, the author chose to present them alongside the evaluation process and results. This approach ensures a clearer overview and improves transparency of the entire evaluation flow for the reader.

5.2.1 Derivation of evaluation criteria for CS frameworks and standards

The evaluation criteria used in the following context-aware scoring method were directly derived from expert interviews and secondary data sources through a structured thematic analysis process. Transcripts from the five semi-structured interviews were manually coded, with codes developed around recurring concepts such as regulatory immaturity, supply chain uncertainty, and institutional fragmentation. These codes were then organized into broader thematic categories, including "regulatory gaps," "vendor origin risks," "governance inconsistency," and "evolving cyber-threat landscape." Through iterative consolidation, the themes were synthesized into six context-sensitive evaluation criteria as presented in Table 3. These criteria were designed to reflect both the strategic cybersecurity needs of planned SMR deployment and the operational constraints identified through expert feedback.

Table 3. Evaluation criteria for scoring.

#	Criterion	Description
1	**Nuclear Sector Specificity**	The degree to which the standard explicitly addresses cybersecurity for nuclear I&C systems, including sector-specific terminology, threat models, and operational contexts.
2	**Supply Chain Security Coverage**	The depth and clarity with which the document addresses third-party risk, vendor assessment, and component origin. Supply chain risks were highlighted in expert interviews and national threat assessments
3	**Alignment with EU Norms**	Whether the framework aligns with EU directives such as NIS2 and CER, and whether its terminology and control structures are compatible with national and EU governance models.
4	**Practical Scalability**	The feasibility of implementation given Estonia's institutional readiness, legal framework, and status as a nuclear newcomer. Includes both administrative and technical scalability, particularly for SMRs.
5	**Governance and Risk Management Guidance**	The presence of clear structures for organizational cybersecurity governance, risk ownership, and accountability—especially important in Estonia's current regulatory vacuum.
6	**Incident Detection and Response Emphasis**	The robustness of the framework's provisions for threat detection, incident response, and recovery. Reflects Estonia's exposure to persistent and hybrid cyber threats.

Expert input also shaped how CS frameworks and standards were interpreted during the scoring process. While each framework or standard was assessed independently using the five-grade scale, interview-derived insights influenced the qualitative judgment applied. For instance, the emphasized concern about the inability to restrict certain vendors by origin under the current procurement law highlighted the importance of supply chain security as a selection criterion. Similarly, stakeholders' emphasis on unclear institutional responsibility led to a more critical evaluation of frameworks with weak governance structures.

This two-level influence, first in defining the evaluation criteria and then in guiding the interpretation of document strengths, ensured that the scoring method remained grounded in the national cybersecurity environment and SMR-specific needs. The resulting evaluation scores presented in section 5.2.4 offer a comparative perspective on how existing international frameworks address Estonia's nuclear cybersecurity challenges.

5.2.2 Selection of frameworks and standards for evaluation

An initial pool of 19 documents was assembled (Appendix 3) based on the literature review, secondary data sources, and their relevance to nuclear, ICS/OT, or critical infrastructure cybersecurity. The next objective was to ensure that the documents kept for final scoring were relevant to the Estonian nuclear context and suitable for expert analysis. The author briefly familiarized himself with the content of documents based on the introduction and scope sections, and by observing the document's structure and references. To limit the selection to a manageable amount, the following inclusion criteria were used:

- direct relevance to nuclear, ICS/OT, or critical infrastructure cybersecurity;
- comprehensive and generally highly recognized security normative;
- presence of risk-contextual priorities such as supply chain security, incident response, and governance;
- The feasibility of analysis in a master's level research effort.

The applied exclusion criteria were:

- outdated publications

- documents with restricted access, requiring purchase
- narrow or generic scope

Despite these criteria, some exceptions in the final selection were still made. As the IEC 62645 is the standard specifically targeting the cybersecurity of NPPs and is widely referenced and suggested in reviewed literature, it was retained for the final scoring despite being commercial and requiring payment [38]. The ISO/IEC 27001 [48], while not targeted specifically to the nuclear or ICS domain, is a globally recognized information system management system (ISMS) standard that is widely referenced in EU, IAEA, and national regulations. Thus, it was retained for final scoring, as well as the NIST CSF 2.0 [48].

After applying all the inclusion and exclusion criteria, a final set of 10 documents was selected as presented in Table 4. These documents were further categorized into three types: technical standards, implementation guidelines, and ISMS or security governance documents. This classification enabled the author to identify the top-scoring document in each category to ensure that all relevant document types were represented in the final recommendation.

Table 4. Selected CS documents for evaluation

Type	Document	Description
Technical standards	IEC 62645:2019	Dedicated international standard for nuclear I&C cybersecurity
	IAEA NSS 33-T	Technical guidance for I&C cybersecurity in nuclear plants
	NIST SP 800-82	Most detailed, publicly available OT/ICS cybersecurity guide
Implementation guidelines	NRC RG 5.71	Official U.S. comprehensice regulatory guide for nuclear CS
	NEI 08-09	CS implementation guide under U.S. NRC oversight
	IAEA NSS 17-T	Guide for national-level integration of CS into nuclear security regimes
	IAEA NSS 42-G	Focused on regulatory CS oversight practices and inspection logic
Governance / ISMS	ISO/IEC 27001	Widely adopted certifiable ISMS framework in nuclear CS
	STUK YVL A.12	National nuclear regulator CS guidance aligned with EU principles
	NIST CSF 2.0	Flexible CS framework for institutional strategy and profile-based maturity planning

5.2.3 Evaluation and scoring of selected CS frameworks and standards

To evaluate the suitability of selected cybersecurity frameworks and standards for the Estonian SMR project context, a structured multi-criteria scoring method was applied. Although not a formal MCDA model, the approach uses multiple predefined criteria scored on a simple scale to support transparent comparison across selected documents. It is specifically tailored to reflect Estonia's cybersecurity threat landscape, regulatory gaps, and institutional maturity as a nuclear newcomer.

This method is justified within the logic of exploratory case study research. Rather than mechanically assessing a document's control coverage, the context-aware evaluation method allows for strategic, risk-informed evaluation, appropriate for Estonia's early-stage SMR program. The derivation of evaluation criteria was detailed in Section 5.2.1.

Each selected cybersecurity framework or standard was independently evaluated against these criteria using a five-point ordinal scale. The scale represents the degree to which each criterion is addressed, based on the content, focus, and operational applicability of the document. Scores were assigned based on the author's structured qualitative judgment, informed by thematic analysis of expert interviews, assessment of the national cyber-threat landscape, and review of secondary data sources. The rationale behind each score is detailed in Table 5.

Individual scores of each criterion were then aggregated to form a cumulative score for each document, supporting comparative analysis. Higher total scores indicate stronger overall suitability for addressing Estonia's SMR program cybersecurity needs within the national regulatory and operational context.

Table 5. Scoring principles by evaluation criterion.

Score	Nuclear Sector Specificity	Supply Chain Security Coverage	Alignment with EU Norms	Practical Scalability	Governance and Risk Management Guidance	Incident Detection and Response Emphasis
5	Entirely nuclear-specific; applicable directly to nuclear facilities	Comprehensive, lifecycle-based supply chain controls (e.g., ISO 27036).	ISO-based, widely referenced in EU law, or authored by EU institutions.	Designed to scale from low- to high-complexity environments. Explicit support for phased / maturity-based adoption.	Fully developed cyber governance model; continuous improvement loop; role clarity.	Full incident lifecycle coverage including technical, procedural, and testing aspects.
4	Covers nuclear use cases but also applicable more broadly.	Strong requirements for vendor risk and procurement integrity.	Not EU-originated but structurally or conceptually fully compatible.	Adaptable with some effort. Graded implementation models included.	Strong on risk and management, but lacking some formal structure.	Strong incident response requirements but limited operational detail.
3	Not nuclear-specific, but used frequently in nuclear sector.	Mentions supply chain but not central or detailed.	Indirectly aligned; may require tailoring or interpretation.	Suitable for mature environments only. Limited scalability.	Governance implied but underdeveloped.	Includes some response principles but lacks structured approach.
2	Generic, sector-neutral; occasionally referenced in nuclear.	Supply chain risk is implied but not addressed directly.	Only partially aligned; not commonly adopted in EU.	Assumes significant institutional maturity. Complex to adapt.	Only technical; governance os out of scope.	Vague mention or assumption of response capability.
1	No relevance to nuclear sector context.	No treatment of supply chain security.	Conflicts with or irrelevant to EU legal models.	Not scalable. Only fits high-capacity national programs.	No treatment of governance or risk planning.	No coverage of detection or response.

Each cybersecurity document included in the final evaluation was reviewed using a structured, criteria-driven process. For documents with full-text access, the analysis began with reading the scope, introduction, and structure to identify where each of the six evaluation criteria was likely addressed. Relevant sections or clauses were then read in detail to conduct informed scoring decisions. For each criterion, a score from 1 to 5 was assigned based on the depth, specificity, and contextual applicability of the guidance provided. When full-text access was unavailable, the evaluation was limited to publicly available summaries, authoritative commentaries, or official cross-reference mapping resources, and such cases were excluded from the final scoring set to maintain consistency. Interpretations were documented in brief analytical summaries to ensure transparency and traceability of the scoring rationale.

To support the evaluation of long or structurally complex standards, GPT-4 was used as a document assistant. Its role was to help identify relevant clauses or sections linked to the six evaluation criteria, especially in standards that were highly technical or lengthy, such as IEC 62645, NRC RG 5.71, or NEI 08-09 [38], [50], [51]. For shorter documents or those with a clear structure, such as ISO/IEC 27001, STUK YVL A.12, the evaluation was done entirely through human reading and annotation. In all cases, the final interpretation and scoring were based on the author's own reading and contextual judgment. AI assistance was used to support document navigation and improve efficiency, not to make scoring decisions.

5.2.4 Evaluation results of selected frameworks and standards

The selected cybersecurity documents were evaluated using a context-aware method across six predefined criteria. The method and criteria descriptions were introduced in detail in the previous two sections. The purpose of this evaluation was to identify which documents offer the most contextually appropriate support for Estonia’s SMR cybersecurity planning.

The following interpretations describe the relative strengths and limitations of each evaluated document:[1]

IAEA NSS 17-T Rev.1 offers implementation-level guidance for integrating computer security into nuclear facility operations. It supports a graded and risk-informed approach aligned with IAEA nuclear security principles, and emphasizes flexibility across development phases. While the majority of its guidance remains conceptual, it outlines core cybersecurity planning and governance functions in ways that might be particularly relevant to regulatory planning in nuclear newcomer contexts. Its supply chain and incident response guidance is general, but suitable for adaptation when paired with more operational documents. The document's scoring results reflect this balance between conceptual scope and practical utility:

Nuclear Sector Specificity (5): The document is entirely nuclear-specific and developed within the IAEA nuclear security framework. It addresses the protection of digital assets in nuclear installations and is intended for use by both operators and national authorities. (Sections 1–2; objective defined in Section 1.1, scope clarified in 1.3).

Supply Chain Security Coverage (3): It refers to procurement, third-party oversight, and system lifecycle considerations but remains general. It lacks concrete models or processes for supplier vetting and integrity assurance. (Section 4.4.1 mentions third-party system considerations; lifecycle elements are broadly referenced in Section 3.3).

Alignment with EU Norms (4): While not EU-authored, it supports principles compatible with EU legislation such as risk-informed governance, graded protection, and the need for coordinated national oversight. (Sections 2 and 3; alignment observable through structural and thematic compatibility with ISO 27001 and NIS2 logic).

Practical Scalability (5): Designed to support a wide range of national capacities, the document is explicitly suited to phased adoption and adaptable implementation strategies—ideal for newcomer states. (Section 3.1.2 outlines flexibility for states with developing capabilities; Annex I offers adaptable functional models).

Governance and Risk Management Guidance (4): NSS 17-T provides a structured view of governance roles and cybersecurity program planning, though continuous

[1] For clarity, a detailed example of how the scoring was conducted is presented for one representative document, including the rationale behind each individual score; all other documents were evaluated using the same criteria and process.

improvement mechanisms and procedural depth are limited. (Section 3.2 and 3.4 discuss responsibilities and oversight; Annex III includes program management considerations).
Incident Detection and Response Emphasis (4): It provides structured guidance on classifying and responding to cybersecurity events. While it does not specify technical tooling or lifecycle logging procedures, it includes clearly defined incident types, procedural responses, and integrates response logic into program design. (Section 3.4 discusses programmatic response responsibilities; Annex IV details event categories and response planning structure).
In summary, IAEA NSS 17-T offers valuable guidance for the countries at early stages of developing nuclear cybersecurity regulation. Its nuclear focus, flexible structure, and emphasis on phased implementation make it well-suited for building institutional understanding and shaping oversight models. However, because it stays at a strategic and conceptual level, it would need to be complemented with more detailed technical standards during later implementation phases [24].

IAEA NSS 33-T provides detailed technical guidance for securing digital I&C systems in nuclear facilities. It outlines a lifecycle approach to system protection, including security zoning, graded controls, and verification of third-party components. The guide is fully nuclear-specific, offering deep relevance for SMR deployment where digital safety systems are integral. While its governance elements are less mature than broader ISMS frameworks, and its supply chain focus is more implicit than contract-driven, it remains one of the most technically precise references for digital I&C cybersecurity [37]. Best used as a system-level security foundation, especially in combination with IEC 62645 and ISO 27001 for broader programmatic and procurement controls.

IAEA NSS 42-G provides guidance to national regulatory bodies on how to oversee computer security in nuclear security regimes. It is written from a regulator's perspective and outlines how cybersecurity requirements should be established, licensed, and inspected. The guide supports graded approaches, performance-based oversight, and integration with broader nuclear security responsibilities. While not highly technical, it appears relevant for regulatory capacity-building in nuclear newcomer states, and due to its general nature, it should be supplemented with more detailed implementation guides [36].

IEC 62645 outlines cybersecurity requirements for I&C systems in nuclear facilities, with a strong focus on lifecycle planning, graded security, and integration with nuclear safety functions. The document is entirely nuclear-specific and technically rigorous. While its structure is demanding and may require adaptation for smaller regulatory teams, it offers targeted controls applicable to digital SMR systems. It appears suitable as a core technical reference in the context of I&C system regulation [38].

STUK YVL A.12 describes the national regulatory expectations for cybersecurity in Finland's nuclear sector. The guide is concise and structured for enforceability, outlining ISMS expectations, auditing intervals, and cyber risk responsibilities for licensees. While specific technical controls are referenced in companion YVL documents, the clarity of institutional roles and procedural requirements makes this document particularly applicable to Estonia's context. The alignment with EU regulatory culture further increases its relevance [18].

ISO/IEC 27001:2022 defines a certifiable ISMS widely used across sectors. The main body of the document describes the organisational context, responsibility assignment, risk treatment processes, and continual improvement cycle. For example, the annex includes controls related to supplier relationship management and cloud service security. Although not nuclear-specific, the document is widely recognized, harmonized with EU legal frameworks, and scalable for use in phased regulatory environments. It appears well-suited to serve as the governance and risk management foundation within a broader regulatory framework [48].

NIST CSF 2.0 is a voluntary framework designed to support scalable cybersecurity governance. It introduces outcome-based functions and profile tailoring that allow for flexibility in national implementation. While not nuclear-specific or directly tied to EU regulation, the framework complements ISO-based systems and appears well-suited for capacity-building in early-phase national programs. Its strong treatment of supply chain risk and outcome-based flexibility makes it a useful strategic overlay for SMR implementation [49].

NIST SP 800-82 Rev. 3 offers detailed technical guidance for securing ICS and OT. The document covers system design, network segmentation, and response preparation in high detail. Though not sector-specific to nuclear, the OT security model seems applicable to

SMR I&C architectures. Governance structures are less formalized, but the document is strong on technical incident detection and response planning. It appears useful as a technical reference for engineering and implementation teams [35].

NRC RG 5.71 Rev. 1 presents detailed cybersecurity guidance for U.S. nuclear licensees, including structured controls, asset classification, and lifecycle planning. Its technical depth and alignment with NEI 08-09 provide a strong implementation model. However, its regulatory structure assumes the U.S. licensing environment, and transposition to the EU context would require substantial adaptation. The guide is especially informative at the technical level, but less applicable for direct regulatory adoption in Estonia [50].

NEI 08-09 Rev. 7 supports licensees in implementing cyber protection programs under U.S. NRC regulation. It includes practical instruction for asset defense and procedural controls, but relies on institutional structures like the CSAT and assumes high compliance capacity. Its strong technical guidance is somewhat offset by assumptions about institutional maturity and regulatory backing. Supply chain risk is addressed indirectly, and scalability concerns lower its direct applicability in Estonia. Still, the document may be used as a reference for implementation rather than regulatory design [51].

In summary, nuclear-specific documents such as IEC 62645, IAEA NSS 33-T, and NSS 17-T scored highest in sector relevance and technical planning, while ISO/IEC 27001 and STUK YVL A.12 demonstrated strong governance, legal compatibility, and scalability. U.S.-origin documents offered implementation depth but often lacked EU regulatory fit.

Based on the cumulative scoring and strategic fit, the four most suitable documents identified for Estonia's SMR cybersecurity framework are:

1) IAEA NSS 17-T Rev.1 " Computer Security Techniques for Nuclear Facilities"
2) IEC 62645:2019 "Nuclear Power Plants I&C Requirements for Security Programs"
3) STUK YVL A.12 "Information Security Management of a Nuclear Facility"
4) ISO/IEC 27001:2022 "Information Security Management Systems – Requirements"

These documents provide a balanced combination of nuclear specificity, programmatic governance, and institutional adaptability. A complete scoring overview, including heatmap visualization, is presented in Table 6.

Table 6. Scoring summary of selected CS regulations and standards.

Type	Document	Nuclear Sector Specificity	Supply Chain Security Coverage	Alignment with EU Norms	Practical Scalability	Governance and Risk Management Guidance	Incident Detection and Response Emphasis	Total Score
Technical standards	IEC 62645:2019	5	4	5	4	4	4	26
	IAEA NSS 33-T	5	4	5	4	4	4	26
	NIST SP 800-82	3	4	2	5	4	5	23
Implementation guidelines	NRC RG 5.71	5	5	3	3	4	5	25
	NEI 08-09	5	3	2	3	4	4	21
	IAEA NSS 17-T	5	3	5	5	4	4	26
	IAEA NSS 42-G	5	3	5	4	4	4	25
Governance / ISMS	ISO/IEC 27001	2	5	5	5	5	4	26
	STUK YVL A.12	5	4	5	4	5	5	28
	NIST CSF 2.0	2	5	4	5	5	5	26

The preceding scoring analysis enables a comparative understanding of the strengths and limitations of each evaluated cybersecurity framework and standard. These results now provide the foundation for a broader strategic discussion, where the implications of document suitability, regulatory gaps, and stakeholder priorities can be synthesized. In the following sections author interprets these findings in the context of Estonia's national cybersecurity posture, institutional readiness, and SMR deployment trajectory.

5.2.5 Qualitative consideration of excluded but relevant standards

ISO/IEC 27036 and the IEC 62443 series were excluded from formal scoring due to reasons of applicability scope and full-text access limitations, respectively, but remain qualitatively relevant to Estonia's nuclear cybersecurity planning [52], [34].

ISO/IEC 27036 provides extensive best-practice guidance for securing supplier relationships, including contractual safeguards, supply chain validation, and cloud procurement assurance. While its sector-neutral scope and generic structure limit its use as a regulatory foundation, it remains highly relevant as a complementary reference,

particularly in the context of high vendor dependency and geopolitical risk exposure in critical infrastructure procurement [52].

The IEC 62443 series, on the other hand, represents the most comprehensive suite of international standards for ICS and OT cybersecurity. Although it is excluded from formal scoring due to paywalled access, its architectural depth and role-based security model have established it as a cornerstone in sectors such as energy, manufacturing, and transportation. Estonia should consider it a long-term supplementary reference, particularly during the later stages of SMR vendor evaluation and integration.

5.2.6 Complementarity of top CS frameworks and standards

The top four documents identified, IEC 62645, IAEA NSS 17-T, STUK YVL A.12, and ISO/IEC 27001, reflect complementary strengths that form a comprehensive foundation for planned SMR cybersecurity posture.

IEC 62645 offers deeply nuclear-specific technical and governance guidance, including design-phase cybersecurity, safety-security coordination, and regulatory expectations.

IAEA NSS 17-T complements this by offering programmatic and lifecycle cybersecurity planning principles, structured for phased adoption by nuclear newcomer states. It is especially useful in contexts where regulatory structures are still forming.

STUK YVL A.12 contributes a regionally and legally aligned governance model, demonstrating how EU-based nuclear regulators integrate cybersecurity into licensing, oversight, and lifecycle management. It provides a structured, enforceable governance reference that Estonia can adopt or adapt.

While NIST CSF 2.0 and ISO/IEC 27001 scored equally in this evaluation, this thesis recommends prioritizing ISO/IEC 27001 due to its international certification status, widespread adoption across EU-aligned jurisdictions, and deeper integration with other ISO-based cybersecurity standards. It also demonstrated the highest performance in the supply chain security criterion. This is especially important given Estonia's reliance on foreign technology vendors and the elevated cyber-threat landscape identified in national security reports. When supplemented with ISO/IEC 27036, the resulting framework offers a highly structured and modular, comprehensive supply chain security architecture, which is essential for safeguarding critical components and service chains in the SMR

context. However, NIST CSF 2.0 remains a valid alternative, providing a highly adaptable, sector-neutral structure that enables organizations to scale their cybersecurity maturity based on evolving risks, making it well-suited for first-time nuclear adopters. Together, these documents bridge the gap between nuclear-specific obligations and broader strategic cybersecurity management practices, offering both operational depth and governance flexibility.

5.3 Recommendations

Building on the previous evaluation and analysis results, this section synthesizes the evaluation results into practical recommendations for the national nuclear cybersecurity strategy, focusing on regulatory foundations, implementation roadmap, and institutional enablers tailored to the SMR implementation context.

5.3.1 Recommended regulatory foundations

Based on the context-aware evaluation results, expert input, and Estonia's national priorities, this thesis recommends a hybrid regulatory model that combines nuclear-specific standards with scalable international governance frameworks.

IEC 62645 and IAEA NSS 33-T form the technical backbone for nuclear I&C system cybersecurity. These offer detailed, lifecycle-oriented control structures aligned with international best practices.

STUK YVL A.12 provides a regionally compatible regulatory model**,** demonstrating how EU-aligned cybersecurity oversight can be embedded into a nuclear licensing regime. It is particularly relevant given the institutional similarities between Estonia and Finland.

IAEA NSS 17-T is recommended as the primary implementation guideline. It offers programmatic guidance, lifecycle planning concepts, and cultural integration principles tailored for nuclear newcomer states and early-phase regulatory planning.

ISO/IEC 27001 is recommended as the strategic governance foundation**,** providing a certifiable Information Security Management System (ISMS) framework that aligns well with EU legal frameworks and critical infrastructure cybersecurity policies.

NIST CSF 2.0 may serve as an alternative or supplementary governance framework due to its scalability and maturity-based architecture.

While excluded from scoring, IEC 62443 series (OT/ICS) and the ISO/IEC 27036 (supply chain) are recommended as supplemental references, especially in later SMR phases.

5.3.2 Implementation roadmap

The following roadmap presents specific, evidence-based recommendations for cybersecurity framework development in the context of Estonia's planned SMR program. Each recommendation is grounded in the findings of this thesis, including the context-aware evaluation results, national legal context, and expert interview insights. Justifications are provided in-line to ensure transparency and traceability of the research data.

Early-stage preparation and strategic planning:

- Estonia should reference ISO/IEC 27001 (or NIST CSF 2.0) in early regulatory planning discussions to explore governance models compatible with its broader cybersecurity ecosystem.
  Justification: These frameworks scored highest for governance maturity and are compatible with Estonia's existing digital policy landscape
- CS requirements should be aligned with the forthcoming Nuclear Energy Act to ensure that digital risks specific to SMR infrastructure are addressed from the outset.
  Justification: There is currently no explicit CS coverage in nuclear legislative drafts. Thus, regulatory gaps must be closed before system design begins.
- Initial collaboration should be established with national CS centers like RIA NCSC-EE[1] or CERT-EE[2], as well as with international nuclear organizations.
  Justification: Interview data emphasized fragmented institutional ownership and the need for early engagement.

[1] https://www.ria.ee/en/cyber-security/national-cyber-security-centre-ncsc-ee
[2] https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee

Regulatory adaptation and framework translation:

- Once Estonia's SMR technology and deployment strategy are clarified, a regulatory mapping exercise should be initiated to evaluate which components of IEC 62645, IAEA NSS 17-T, and STUK YVL A.12 are most applicable to Estonia's national context.

  Justification: These scored highest in evaluation and reflect both nuclear specificity and EU compatibility.
- Guidance should be prepared to support future vendor assessment, procurement control, and architecture-level cybersecurity planning.

  Justification: Interviewees emphasized risks in vendor control and limitations in national procurement law.

  ISO/IEC 27036 should be used as a reference in the formulation of non-binding guidelines to manage supply chain cybersecurity risks.

  Justification: This standard is widely recognized in literature for its relevance in addressing supply-chain, third-party, and procurement risks.

Capacity building and institutional preparedness:

- Training and technical cooperation should be initiated with experienced nuclear cybersecurity actors, such as Finland, Canada, the U.S., and the IAEA.

  Justification: Experts unanimously identified the shortage of nuclear-specific CS capacity as a major weakness.
- Cybersecurity governance should be explicitly included in the mandate of any future regulatory institution responsible for nuclear oversight.

  Justification: Interviews revealed concerns over unclear institutional responsibilities.

This roadmap ensures cybersecurity readiness evolves in tandem with Estonia's nuclear program and regulatory maturity.

5.3.3 Institutional and legal enablers

The success of this cybersecurity strategy depends on Estonia addressing key institutional and legal gaps:

- The Estonian government should clarify which institution will be responsible for cybersecurity oversight in the nuclear sector, whether by assigning the task to an existing authority or by creating a new regulator.
  Justification: Experts' concerns over institutional ambiguity and the risk of delayed responsibility assignment.
- Supply chain and vendor cybersecurity risks should be elevated to a national policy priority.
  Justification: This issue was repeatedly raised in interviews as a structural vulnerability, particularly considering legal limitations in excluding high-risk vendors.

These recommendations reflect Estonia's position as a digitally capable newcomer to nuclear energy. While the SMR project is still in early stages, the proposed actions offer a practical foundation for regulatory planning. As the program evolves, they should be revisited in light of future legal, technical, and institutional developments.

6 Validation

The objective is to validate the findings and recommendations developed during the study. Given the qualitative and exploratory nature of the research, validation is focused on ensuring credibility, contextual relevance, and practical applicability of the results rather than statistical generalizability.

To achieve this, the study employs expert validation through follow-up interviews with key stakeholders from the Estonian cybersecurity and energy sectors. The selected experts include representatives from public authorities and industry experts who were previously involved in national nuclear planning or interviewed earlier in the research.

6.1 Validation results

The interviewees were given the chance to review the thesis results extract sent one working day prior. The interviews took place between 6-8 May 2025. The planned length of the interviews was 30 minutes. The longest interview lasted 43 minutes, and the shortest interview lasted 34 minutes. Interviews were conducted in Estonian, recorded and then transcribed. The interviewees are listed in Table 7.

Table 7. Interviewees of validation interviews

Organization	Role in SMR process	Job position	Sectoral expertise
Fermi Energia	SMR's licensee; operator	Chief Technology Officer	Nuclear energy and power plants
RIA	Critical infrastructure CS expertise, advisory in CS matters	Cybersecurity Centre of Critical Infrastructure, head of tech. department	Critical infrastructure and vital services cybersecurity
Minsitry of Interior	Nuclear security expertise, nuclear policy development	Nuclear Security and Emergency Preparedness advisor	Nuclear security, safety and safeguards; nuclear regulations

All interview participants agreed that the evaluation criteria used in this study accurately reflect Estonia's current context, particularly the cybersecurity challenges and institutional needs involved in implementing a nuclear program based on SMR technology.

None of the experts proposed any additions or corrections to the top-rated standards. The strong performance of the Finnish national regulator's standard STUK YVL A.12 received notable attention, and its relevance for Estonia was emphasized as especially well aligned. More broadly, most interviewees acknowledged limited familiarity with nuclear-sector cybersecurity standards. In this respect, the consolidated set of frameworks and standards presented in this study was considered a valuable contribution.

Two additional questions were raised during the interviews: one expert asked why Estonia's national information security standard E-ITS was not included in the comparison; another inquired whether ISO 19443 was considered. Both of these points are addressed by the author in the Discussion section [53], [54].

All participants supported the proposed phased implementation approach and the idea of combining multiple regulatory frameworks. The strategy of integrating both nuclear-specific and general IT governance standards into a hybrid regulatory foundation was seen as reasonable and contextually appropriate.

Regarding institutional and legal structures, the interviewees largely agreed with the conclusion that responsibilities within Estonia's future nuclear governance remain undefined. Several different institutional options were proposed for housing the cybersecurity oversight function. Some suggested that this function could be embedded within the future nuclear regulatory body; others proposed placing it within an existing authority. The RIA was most frequently mentioned, as it currently acts as the national cybersecurity competence center. Other candidates included the Technical Regulatory Authority (TTJA) or the Ministry of Justice and Digital Affairs.

As an additional recommendation, one expert proposed that any future SMR training center or environment in Estonia should explicitly include cybersecurity capabilities. Specifically, it should be designed to support simulation and virtual training for IT security incidents, and this consideration could also be reflected in the SWOT framework.

In conclusion, the evaluation criteria were considered appropriate and well-matched to Estonia's conditions. There were no objections to the methodology or results. The recommended standards were viewed as mutually complementary and collectively sufficient to cover the full range of assessment criteria. While E-ITS and ISO 19443 were

raised as possible additions, the core proposal was widely supported. The phased implementation strategy and hybrid regulatory model were both seen as highly suitable. The only area that prompted extensive discussion was the institutional responsibility for cybersecurity oversight, where multiple governance pathways remain open.

As a result of the evaluation interviews, no further changes were required to the proposed research results.

7 Discussion

In this chapter, the author reflects on the findings of the study, drawing connections to earlier research, expert perspectives, and Estonia's context. It considers the implications of the results and discusses observations from the validation process.

7.1 Comparison with prior study

One of the earliest public efforts to compare nuclear cybersecurity standards was conducted by Eve Hunter in her 2016 master's thesis at TalTech [26]. This study shares a foundational motivation with her thesis, *"A Comparative Analysis of Cybersecurity Guidelines and Standards for Nuclear Power Plants."* Both aim to address the fragmented landscape of cybersecurity documents applicable to the nuclear sector. However, the differences in methodology, document selection, national context, and intended outcomes highlight the evolution of regulatory thinking over the past decade and the specific needs of newcomer nuclear states like Estonia.

Methodological Scope and Drivers:

Hunter's study was driven by an intent to benchmark how well various cybersecurity standards mapped to the NIST Cybersecurity Framework (CSF), using a static document-to-subcategory mapping method. She applied this matrix to nine publicly available documents and used expert validation and statistical analysis (including ANOVA) to verify internal consistency.

In contrast, the present study applies a context-aware evaluation method designed specifically for Estonia's newcomer nuclear status. Rather than mapping to CSF categories, this thesis evaluates each document across six qualitative criteria reflecting national institutional capacity, legal compatibility, governance maturity, and implementation scalability. The approach is grounded in cybersecurity governance literature and risk-informed regulatory principles, aiming not to benchmark control completeness but to guide real-world regulatory adaptation.

Document Selection and Overlap:

Hunter evaluated nine documents, including ISO/IEC 27001, NEI 08-09, NRC RG 5.71, NIST SP 800-53, NIST SP 800-82, IAEA NSS 17, ISA/IEC 62443-2-1/3-3, NERC CIP v5, and WINS 4.3 [26]. Several of these are included in the present thesis as well, most notably ISO/IEC 27001, NEI 08-09, NRC RG 5.71, and NIST 800-82. However, Hunter's

list leans more heavily toward documents from the U.S. and electricity sector context (e.g., NERC CIP), and includes documents that are paywalled (ISA/IEC 62443) without addressing access limitations.

In contrast, this thesis applies strict document inclusion criteria based on accessibility, nuclear relevance, and alignment to the national context. Regional sources such as STUK YVL A.12 and harmonized standards like IEC 62645 are also incorporated to reflect the EU context.

Results Comparison and Similarities:

Despite methodological differences, both studies converge on a key outcome: no single document sufficiently addresses the cybersecurity needs of nuclear installations. Both recommend a hybrid solution. Hunter recommends combining NEI 08-09 and ISO/IEC 27001 alongside NIST CSF. Similarly, this thesis recommends a composite of IEC 62645, IAEA NSS 17-T, ISO/IEC 27001, and STUK YVL A.12, balancing nuclear specificity, institutional feasibility, and governance scalability.

Document-level results also show notable overlap. ISO/IEC 27001, NRC RG 5.71, and NEI 08-09 are identified in both studies as key contributors, though their strengths are interpreted differently. In Hunter's matrix, scoring is tied to the presence of CSF subcategory coverage. In this thesis, documents like NEI 08-09 and NRC RG 5.71 scored lower in scalability or legal fit, despite their technical depth.

Role of Expert Interviews:

Another important distinction lies in the treatment of expert interviews. Hunter used interviews with five U.S.-based experts mainly to validate her mapping outcomes. These interviews were not thematically analyzed and did not directly influence the document scoring or selection model.

In contrast, this study applies methodological triangulation, using interviews to help formulate evaluation criteria, validate document selection, and interpret strategic relevance. The input of Estonian stakeholders, including national authorities and cybersecurity experts, played a critical role in grounding the analysis and recommendations in the local institutional context.

Relevance and Transferability:

Hunter's work remains valuable for benchmarking purposes in mature regulatory environments or operator-level implementation. However, its methodology lacks adaptability for phased national regulation or nuclear newcomer contexts. By contrast, this study aims to directly support policy design and regulatory preparation in Estonia.

The emphasis is on feasibility, scalability, and institutional integration, not just technical alignment.

In summary, while Hunter's thesis laid important groundwork in the systematic evaluation of nuclear cybersecurity documents, this study builds upon and diverges from it to reflect the governance and risk realities of a national SMR program in its early stages. Together, they form a useful continuum – from benchmarking toward context-specific regulatory design.

7.2 Considerations from validation interviews

Treatment of the national E-ITS Standard

During the validation interviews, the exclusion of the national Estonian Information Security Standard (E-ITS) from the scoring set was raised [53]. While E-ITS is a nationally adopted ISMS framework derived from ISO/IEC 27001 and Germany's BSI IT-Grundschutz[1], its scope and language accessibility present limitations for inclusion in an international nuclear context. E-ITS is published only in Estonian and is not widely recognized beyond Estonia's borders. Furthermore, given the global nature of nuclear security regulation, cybersecurity frameworks applicable to nuclear systems must be internationally harmonized, certifiable, and aligned with IAEA and EU regulatory expectations. For these reasons, E-ITS was excluded from the evaluated set, although its principles may still be indirectly relevant where national implementation of ISO/IEC 27001 is planned.

Consideration of ISO 19443 in the context of this study

Another interesting observation during the validation interview process was the potential relevance of ISO 19443, which was raised by an interviewee as an additional standard worth evaluating. ISO 19443:2018 is a quality management system standard developed specifically for suppliers in the nuclear sector [54]. It builds upon ISO 9001 and introduces nuclear-sector-specific requirements for ensuring product and service conformity, including aspects of traceability, safety culture, and supplier oversight.

[1] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

While at first sight it might seem relevant for the study by ensuring quality assurance and compliance in nuclear supply chains, ISO 19443 was not included in the formal evaluation in this thesis. Primarily because the focus of the study was on cybersecurity frameworks, standards, and governance models, whereas ISO 19443 is a quality assurance standard without dedicated cybersecurity provisions. Nevertheless, ISO 19443 may play a complementary role in future regulatory development for Estonia's SMR program, especially when establishing procurement policies, contractor qualification procedures, and traceability systems.

7.3 The importance of EU legal alignment in the evaluation process

As an EU member, Estonia must ensure that any cybersecurity framework adopted for its SMR program aligns with Union law, particularly the NIS2 Directive and the Estonian Cybersecurity Act [55]. These instruments mandate structured risk management, incident handling, supply chain oversight, and institutional accountability for essential service providers, including in the energy sector.

Within this legal environment, including "EU norm alignment" as an evaluation criterion was therefore necessary. Some technically strong documents, such as NRC RG 5.71 and NEI 08-09, were scored lower in this area due to their close integration with U.S.-specific legal and institutional models. These frameworks assume federal licensing structures, licensee autonomy, oversight practices, and U.S.-specific terminology that differ significantly from EU norms, making them difficult to transpose without major adaptation.

In contrast, ISO/IEC 27001 and STUK YVL A.12 scored 5 for EU alignment, reflecting their structural compatibility with EU regulatory expectations. ISO/IEC 27001 is directly referenced in many EU legal instruments, while STUK’s guidance reflects similar institutional principles close to Estonia's and the EU governance models.

Some might argue that technically advanced documents should determine suitability. However, in the particular case, where the regulatory foundation is still being developed, legal alignment is not optional. Choosing documents that are technically sophisticated but lack EU compatibility could delay regulatory development or create compliance gaps. Lower scores of certain U.S. origin documents on the EU alignment criterion are not a

dismissal of their quality, but a realistic reflection of their limited legal and institutional transferability. Including this criterion ensured that the selected frameworks were not only technically sound but also actionable within Estonia's legal and governance model.

7.4 The risk of ignoring cybersecurity in early-stage planning

This study was carried out at a time when cybersecurity is almost entirely absent from Estonia's public nuclear energy planning. While energy policy, legal structures, and safety culture are being discussed in national nuclear working group reports and government documents, cybersecurity has received only minor mention, usually in brackets or footnotes. This is not just an Estonian issue. Across the energy sector more broadly, cybersecurity is often seen as a technical detail to be addressed later, not a strategic concern to be built in from the start. This thesis challenges that approach.

The findings support the view that cybersecurity is not something that can be retrofitted after the primary object, system, or structure is built – it has to be considered from the beginning. If cybersecurity aspects are left out of early planning decisions about licensing, oversight, procurement, and digital systems, it becomes much harder to fix those gaps later. Delaying cybersecurity integration leads to fragmentation, unclear responsibilities, and weaker overall resilience.

Several expert interviewees confirmed this risk. They noted that cybersecurity is not currently part of Estonia's nuclear policy discussions, and no clear authority has been assigned to oversee it. The main explanation offered is that it is still too early in the process, and that more fundamental issues must be addressed first. While this might be understandable, it overlooks the reality that digital components, systems, services, information, and even people introduce cybersecurity risks at every phase of a program. Awareness of these risks needs to be embedded from the outset, even in the most abstract or high-level planning stages. This matches what the author found in Estonia's Nuclear Energy Working Group report, where cybersecurity is not addressed as a structural topic. That gap is what led to the development of a document selection and evaluation method tailored to Estonia's current starting point and institutional capacity.

The broader lesson is clear – for any newcomer state preparing for nuclear energy, cybersecurity must be treated as an equally important issue, not just a technical one. It requires attention at the regulatory, institutional, and planning levels. This thesis presents

cybersecurity as a governance responsibility. Bringing it into Estonia's SMR planning now would not only strengthen national preparedness, but it could also offer a model for other countries facing similar challenges.

At the same time, it is important to acknowledge that the evaluation conducted in this study and the proposed hybrid cybersecurity framework reflect the regulatory and institutional conditions in effect at the time of writing. Over the coming years, both EU and national legislation may evolve, and new cybersecurity regulations specifically targeting SMRs may emerge. Given the long timeline until the planned commissioning of Estonia's first SMR, continuous monitoring of legislative developments and regulatory guidance will be essential. In parallel, lessons learned from international reference projects, such as Canada's Darlington SMR deployment[1], will provide valuable input for refining Estonia's cybersecurity posture. This thesis should therefore be seen as a foundational contribution rather than a final verdict, offering a structured starting point for ongoing regulatory adaptation.

[1] https://fermi.ee/bwrx-300-sai-kanadas-ehitusloa/

8 Limitations and future work

The chapter summarises the main limitations of the study and reflects on how they shaped the scope and methods. It also outlines potential directions for future research as Estonia's SMR programme and regulatory framework continue to evolve.

8.1 Limitations

As with any academic study and evaluation, several limitations must be acknowledged. Access to data was restricted by the sensitivity of the subject matter. Specific technical and security-related details of nuclear plant projects are often classified, limiting the analysis to publicly available sources. For example, the publicly released report of the Estonian Nuclear Energy Working Group omits cybersecurity considerations. It is known to the author that security-related aspects were evaluated, likely under a confidential annex not accessible for academic analysis. This confidentiality constraint introduces a blind spot, particularly in assessing Estonia's actual regulatory planning regarding nuclear cybersecurity.

Due to the limited global deployment of SMRs, there is a scarcity of empirical data on real-world cybersecurity challenges and practices. Only two SMRs are currently operational globally, one in China and one in Russia. As a result, existing research is mostly conceptual, exploratory, or vendor-driven, rather than based on post-implementation assessment.

A significant part of cybersecurity standards and regulatory guidelines, particularly those issued by proprietary bodies, were inaccessible due to purchase or subscription demand. Although the author conducted a broad listing, many relevant standards had to be excluded from evaluation due to financial constraints. Despite this, exceptionally important documents, such as IEC 62645, were procured to ensure that the most critical nuclear-specific guidance was included.

Finally, while the context-aware evaluation method enabled flexibility and context sensitivity, it is ultimately a qualitative and judgment-based technique, not a formal quantitative decision model. Although scores were derived transparently and informed by

expert feedback and literature, the absence of numeric weighting or sensitivity testing limits the granularity of comparison between frameworks.

Despite these limitations, the overall validity of the findings was preserved. Where direct access to proprietary standards was limited, the analysis relied on secondary data analysis – verified clause-level summaries and publicly available references. While the scoring method was qualitative, it was transparently applied and ensured by structured document review, allowing meaningful comparison despite the absence of numeric modeling.

8.2 Future research directions

As Estonia develops its national nuclear regulatory framework, follow-up research should evaluate how the proposed hybrid CS regulatory baseline model performs in practice, particularly during vendor assessments, system integration, and regulatory inspections.

Another possible direction is to carry out cross-national regulatory comparison studies in the future. As more SMRs enter licensing phases globally, comparative studies of nuclear cybersecurity governance (e.g., in Finland, Canada, South Korea, and Poland) could yield transferable lessons for small and emerging nuclear states.

9 Summary

This thesis set out to identify which cybersecurity frameworks and standards are most suitable to support the secure implementation of Estonia's first SMR. It also examined the key cybersecurity challenges Estonia must address as a nuclear newcomer.

To address this research problem, the study employed an exploratory case study methodology, triangulating evidence from peer-reviewed literature, publicly available standards and regulatory documents, and semi-structured expert interviews with national stakeholders. A risk-contextual approach was applied to define evaluation criteria that reflect Estonia’s specific threat environment, regulatory capacity, and nuclear infrastructure needs. These criteria then formed the basis for the context-aware evaluation, in which selected cybersecurity frameworks and standards were scored and ranked accordingly.

The results indicate that a hybrid approach, combining nuclear-specific technical standards and guidance from IEC 62645, IAEA NSS 17-T, and the national regulatory guide STUK YVL A.12 with internationally accepted cybersecurity governance standards like ISO/IEC 27001, offers the most promising foundation for Estonia's SMR cybersecurity framework. These documents together provide scalable, certifiable, and EU-compatible bases for national regulation.

The research also identified several critical cybersecurity challenges for the SMR program, including:

- Limited availability of nuclear-specific cybersecurity expertise;
- Elevated supply chain risk due to geopolitical constraints;
- Gaps in the current legal framework regarding nuclear regulation;
- Potential for targeted influence operations and insider threats.

Despite access limitations to some proprietary standards and the small expert sample size, the thesis delivers actionable recommendations grounded in contextual evidence. These include prioritizing cybersecurity-by-design practices, developing human capital in nuclear cybersecurity, and aligning national regulation with the most relevant and scalable international frameworks.

This thesis set out to determine which cybersecurity frameworks and standards would best support Estonia as it prepares to implement an SMR. The first main research question, on how to identify suitable cybersecurity standards, was addressed by designing an evaluation method that accounted for both technical content and Estonia's regulatory starting point. Sub-questions about international practice (SRQ1) and evaluation criteria (SRQ2) were covered through the document review, clause-based analysis, and expert triangulation. The second main research question (MRQ2), regarding Estonia's specific cybersecurity challenges, was explored through interviews and secondary data analysis.

The thesis answered all established research questions and delivered a set of practical recommendations tailored to Estonia's position as a nuclear newcomer.

In conclusion, the study offers a defensible and flexible strategy for integrating cybersecurity into Estonia's emerging nuclear program. It provides a baseline for regulatory planning and lays the groundwork for further academic and institutional exploration in the field of nuclear cybersecurity in newcomer countries.

References

[1] B. Aamoth, W. E. Lee, and H. Ahmed, “Net-Zero Through Small Modular Reactors - Cybersecurity Considerations,” in *IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society*, Brussels, Belgium: IEEE, Oct. 2022, pp. 1–5. doi: 10.1109/IECON49645.2022.9968304.

[2] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, “Ukraine cyber-induced power outage: Analysis and practical mitigation strategies,” in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, IEEE, Apr. 2017, pp. 1–8. doi: 10.1109/CPRE.2017.8090056.

[3] B. Thomas, “Cyber-Attack on Indian Nuclear Power Plant Exposes Threat of ‘Snooping’ Malware,” Nov. 2019. Accessed: May 18, 2025. [Online]. Available: https://www.bitsight.com/blog/cyber-attack-on-indian-nuclear-power-plant-exposes-threat-of-snooping-malware

[4] “Varustuskindluse aruanded ja konverentsid Elering.” [Online]. Available: https://www.elering.ee/varustuskindluse-aruanded-ja-konverentsid

[5] Tuumaenergia töörühm, “Tuumaenergia kasutuselevõtmise võimalused Eestis,” Dec. 2023. [Online]. Available: https://kliimaministeerium.ee/sites/default/files/documents/2023-12/Tuumaenergia töörüham lopparuanne.pdf

[6] “Cyber Security in Estonia 2024,” 2024. [Online]. Available: https://ria.ee/sites/default/files/documents/2024-02/Cyber-security-in-Estonia-2024.pdf

[7] “IAEA Milestones Guidance Updated to Include Considerations for SMRs,” Aug. 2024. [Online]. Available: https://www.iaea.org/newscenter/news/iaea-milestones-guidance-updated-to-include-considerations-for-smrs

[8] U. C. Arinze, O. B. Longe, and A. H. Eneh, “Regulatory Perspective on Nuclear Cyber Security: The Fundamental Issues,” *International Journal of Nuclear Security*, Jul. 2020, doi: 10.7290/ijns060103.

[9] “Elering Live.” [Online]. Available: https://dashboard.elering.ee/en

[10] V. G. Ferreira, “Strategic autonomy and the future of nuclear energy in the EU,” Feb. 2024. Accessed: May 18, 2025. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757796/EPRS_BRI(2024)757796_EN.pdf

[11] “Small Modular Reactors explained - European Commission.” [Online]. Available: https://energy.ec.europa.eu/topics/nuclear-energy/small-modular-reactors/small-modular-reactors-explained_en

[12] “BWRX-300 General Description,” 2023, *GE-Hitachi Nuclear Energy Americas LLC*.

[13] A. Ayodeji, M. Mohamed, L. Li, A. Di Buono, I. Pierce, and H. Ahmed, “Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors,” *Progress in Nuclear Energy*, vol. 161, p. 104738, Jul. 2023, doi: 10.1016/j.pnucene.2023.104738.

[14] N. Chowdhury, “CS Measures for Nuclear Power Plant Protection: A Systematic Literature Review,” *Signals*, vol. 2, no. 4, pp. 803–819, Dec. 2021, doi: 10.3390/signals2040046.

[15] “Nuclear Sector Cybersecurity Framework Implementation Guidance CISA,” Jan. 2021, *Cybersecurity and Infrastructure Security Agency*. [Online]. Available: https://www.cisa.gov/resources-tools/resources/nuclear-sector-cybersecurity-framework-implementation-guidance

[16] “NIS2 Directive (EU) 2022/2555 of the European Parliament and of the Council,” 2022. Accessed: May 18, 2025. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/2022-12-27

[17] “CER Directive (EU) 2022/2557 of the European Parliament and of the Council,” Dec. 14, 2022. Accessed: May 18, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

[18] Radiation and Nuclear Safety Authority (STUK), *Information Security Management of a Nuclear Facility*, Guide YVL A.12, Helsinki, Finland, 2021.

[19] “International Security and Estonia 2025,” 2025. Accessed: May 18, 2025. [Online]. Available: https://www.valisluureamet.ee/doc/raport/2025-en.pdf

[20] “Cyber Security in Estonia 2025,” 2025. Accessed: May 18, 2025. [Online]. Available: https://www.ria.ee/sites/default/files/documents/2025-02/Cyber-security-in-Estonia-2025.pdf

[21] “Annual Review 2024- 2025,” 2025. Accessed: May 18, 2025. [Online]. Available: https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf

[22] “International Security and Estonia 2024,” 2024. Accessed: May 18, 2025. [Online]. Available: https://www.valisluureamet.ee/doc/raport/2024-en.pdf

[23] “Enereetikasektori Küberriskianalüüs,” 2024. Accessed: May 18, 2025. [Online]. Available: https://www.ria.ee/sites/default/files/documents/2024-06/energeetikasektori-kuberriskianaluus-2024.pdf

[24] International Atomic Energy Agency, *Computer Security Techniques for Nuclear Facilities*, IAEA Nuclear Security Series No. 17-T (Rev. 1), Vienna, Austria, 2021.

[25] International Organization for Standardization and International Electrotechnical Commission, *Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks*, ISO/IEC 27005:2022, Geneva, Switzerland, 2022.

[26] E. Hunter, “A Comparative Analysis of Cybersecurity Guidelines and Standards for Nuclear Power Plants,” TalTech, Tallinn, 2016.

[27] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering – A systematic literature review,” *Inf Softw Technol*, vol. 51, no. 1, pp. 7–15, Jan. 2009, doi: 10.1016/j.infsof.2008.09.009.

[28] P. Sabharwall *et al.*, “Cyber security for microreactors in advanced energy systems,” *Cyber Security: A Peer-Reviewed Journal*, vol. 4, no. 4, p. 345, Jun. 2021, doi: 10.69554/YWJS7812.

[29] K. Chung, K. J. Lee, Y. J. Choo, Y. K. Choi, and S. Y. Jo, “Cyber-Security Considerations for SMRs to Conduct Load-following Operations in Korea,” 2023.

[30] Yoon Ki Choi, Kyung Jin Lee, Yeon Jun Choo, and Kiwhan Chung, “Cyber security considerations for technologies intended in the future SMR,” May 2023. [Online]. Available: https://www.kns.org/files/pre_paper/49/23S-526-%EC%B5%9C%EC%9C%A4%EA%B8%B0.pdf

[31] R. Fasano, “Cyber Risks To The Operational Technology Architectures Of Next Generation Nuclear Reactors,” in *Proposed for presentation at the 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC & HMIT 2021) held June 14-17, 2021.*, US DOE, Jun. 2021. doi: 10.2172/1873274.

[32] R. Duguay, “Small modular reactors and advanced reactor security: Regulatory perspectives on integrating physical and cyber security by design to protect against malicious acts and evolving threats,” 2021, *University of Tennessee Institute for Nuclear Security*. doi: 10.7290/ijns070102.

[33] S. Eggers, R. Youngblood Iii, M. Overlin, R. Li, J. Mahanes, and K. Le Blanc, “Digital Engineering and Cybersecurity Decision Analysis in Early Phases of SMR-Driven IES Projects,” Sep. 2023. doi: 10.2172/2246624.

[34] International Electrotechnical Commission, *Security for Industrial Automation and Control Systems – Series*, IEC 62443, Geneva, Switzerland, various dates.

[35] National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82 Revision 3, Gaithersburg, MD, USA, Sep. 2023.

[36] International Atomic Energy Agency, *Computer Security Incident Response Planning at Nuclear Facilities*, IAEA Nuclear Security Series No. 42-G, Vienna, Austria, 2021.

[37] International Atomic Energy Agency, *Computer Security of Instrumentation and Control Systems at Nuclear Facilities*, IAEA Nuclear Security Series No. 33-T, Vienna, Austria, 2018.

[38] International Electrotechnical Commission, *Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity Requirements*, IEC 62645:2019, Geneva, Switzerland, 2019.

[39] International Electrotechnical Commission, *Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Coordinating Safety and Cybersecurity*, IEC 62859:2016 + AMD1:2019, Geneva, Switzerland, 2019.

[40] J. Linnosmaa, T. Malm, A. Kotelb, and J. Pärssinen, "Survey of cybersecurity standards for nuclear I&C systems," Nov. 2021. Accessed: May 18, 2025. [Online]. Available: https://cris.vtt.fi/files/53942179/Linnosmaa_ISOFIC_2021.pdf

[41] Cristina Siserman-Gray and Guy Landine, "Cybersecurity for small modular reactors (SMRs): Regulatory challenges and opportunities," 2023.

[42] A. Ayodeji, A. Di Buono, I. Pierce, and H. Ahmed, "Wavy-attention network for real-time cyber-attack detection in a small modular pressurized water reactor digital control system," *Nuclear Engineering and Design*, vol. 424, Aug. 2024, doi: 10.1016/j.nucengdes.2024.113277.

[43] Robert K. Yin, *Case Study Research and Applications: Design and Methods*. London, England: SAGE Publications, 2018.

[44] John W. Creswell and J. David Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 6th ed. SAGE Publications, 2022. [Online]. Available: https://uk.sagepub.com/en-gb/eur/research-design/book270550

[45] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qual Res Psychol*, vol. 3, no. 2, pp. 77–101, Jan. 2006, doi: 10.1191/1478088706qp063oa.

[46] U. Flick, Ed., *A companion to qualitative research*, Repr. Los Angeles: SAGE, 2004.

[47] M. A. Benzaghta, A. Elwalda, M. Mousa, I. Erkan, and M. Rahman, "SWOT analysis applications: An integrative literature review," *Journal of Global Business Insights*, vol. 6, no. 1, pp. 55–73, Mar. 2021, doi: 10.5038/2640-6489.6.1.1148.

[48] International Organization for Standardization and International Electrotechnical Commission, *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*, ISO/IEC 27001:2022, Geneva, Switzerland, 2022.

[49] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST Cybersecurity White Paper 29, Gaithersburg, MD, USA, Feb. 2024.

[50] U.S. Nuclear Regulatory Commission, *Cyber Security Programs for Nuclear Power Reactors*, Regulatory Guide 5.71 Revision 1, Washington, DC, USA, Feb. 2023.

[51] Nuclear Energy Institute, *Cyber Security Plan for Nuclear Power Reactors*, NEI 08-09 Revision 7, Washington, DC, USA, Feb. 2024.

[52] International Organization for Standardization and International Electrotechnical Commission, *Information Security, Cybersecurity and Privacy Protection – Supplier Relationships – Part 3: Guidelines for Information and Communication Technology Supply Chain Security*, ISO/IEC 27036-3:2023, Geneva, Switzerland, 2023.

[53] Estonian Information System Authority, *Information Security Standard (E-ITS)*, Version 3.6, Tallinn, Estonia, 2022. (In Estonian)

[54] International Organization for Standardization, *Quality management systems – Specific requirements for the application of ISO 9001:2015 by organizations in the supply chain of the nuclear energy sector*, ISO 19443:2018, Geneva, Switzerland, 2018.

[55] Riigikogu, *Cybersecurity Act (KüTS)*, RT I, 22.05.2018, 1, Estonia, 2018.

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

I, Andres Pelešev

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis, "Cybersecurity Regulatory Challenges in Small Modular Reactor Implementation: A Case Study of Estonia" supervised by Silvia Lips and Shaymaa Mamdouh Khalil
2. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
3. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
4. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
5. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

15.05.2025

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Expert interview questions in Estonian and English

Interview questions in Estonian

Q.1. Palun tutvusta, Milline on Sinu tööpositsioon ja põhivastutusvaldkond?

Q.2. Kirjelda palun oma senist kogemust küberturvalisuses ja/või tuumaenergeetikas.

Q.3. Millised on olnud varasemad kokkupuuted küberturvalisusega uute energiatootmisrajatiste rakendamisega sh. tuumarajatised?

Q.4. Millised on teadaolevad parimad turvalisuse praktikad tuumajaamade rajamisel maailmas?

Q.5. Millised on olulisemad turvalisusega seotud regulatsioonid või standardid (sh küberturvalisuse) energeetika valdkonnas?

Q.6. Kuidas energiatootmisrajatiste rakendamisel Eestis on seni arvestatud Security by Design põhimõttega (ennekõike küberturvalisuse aspektist)?

Q.7. Kuidas uute energiatootmisrajatiste planeerimisel ja rakendamisel selgitatakse ja ennetatakse võimalikke tööstusjuhtsüsteemide (ICS) ja/või küberfüüsilisi (cyber-physical) ohtusid?

Q.8. Millised on peamised erisused NPP-de rakendamisel võrreldes teiste energiatootmisrajatiste rakendamisega turvalisuse aspektist (sh CS)?

Q.9. Kuidas hindad Eesti tänast valmisolekut ja võimekust CS aspektist NPP-de rakendamiseks?

Q.10 Kuidas hindad Eesti tänast valmisolekut ja võimekust regulatiivsest aspektist NPP-de rakendamiseks?

Q.11. Kuidas hindad Eesti tänast valmisolekut ja võimekust organisatoorsest aspektist NPP-de rakendamiseks?

Q.12. Milliseid aspekte pead selle juures kõige kriitilisemaks NPP juurutamisel Eestis?

Q.13. Millised on teadaolevad olulisimad CS väljakutsed NPP-de juurutamisel maailmas?

Q.14. Millised võivad olla kõige tõenäolisemad ründed vastjuurutatud (või juurutamisel oleva) Eesti NPP vastu?

Q.15. Millised on Sinu hinnangul täna Eesti tugevused ja/või eelised NPP rajamisel?

Q.16. Kas on midagi, mida sooviksid veel lisada?

Q.17. Millist eksperti soovitaksid selle teema osas veel intervjueerida?

Interview questions in English

Q.1. What is your current position and main responsibilities?

Q.2. Please describe your experience in cybersecurity and/or nuclear energy.

Q.3. What have been the previous experiences with implementing CS in power plants, including NPPs?

Q.4. What are the known best security practices in constructing NPPs?

Q.5. What are the most important CS-related regulations or standards in the energy sector?

Q.6 How has the Security by Design principle been considered in implementing power plants in Estonia so far?

Q.7. How are potential ICS threats identified and mitigated in the planning and implementation of new power plants?

Q.8. What are the main differences between the implementation of NPPs and the implementation of other power plant types from a security perspective (including CS)?

Q.9. How do you rate Estonia's current readiness and capability from a CS perspective for implementing NPPs?

Q.10 How do you rate Estonia's current readiness and capability from a regulatory perspective for implementing NPPs?

Q.11. How do you rate Estonia's current readiness and capability from an organizational perspective for implementing NPPs?

Q.12. What aspects do you consider to be the most critical in implementing NPP in Estonia?

Q.13. What are the most critical CS challenges in implementing NPPs worldwide?

Q.14. What could be the most probable attacks against the newly implemented (or during the implementation process) Estonian NPP?

Q.15. What are Estonia's strengths and/or advantages in establishing NPPs today?

Q.16. Is there anything you would like to add?

Q.17. Do you recommend any additional expert to be interviewed?

Appendix 3 – Identified CS frameworks and standards

Identificator	Title	Published	Issuer	Included (Y/N) / reason
NIST CSF 2.0	The NIST Cybersecurity Framework (CSF) 2.0	Feb 2024	NIST, U.S.	Yes / widely referenced
IST SP 800-82 Rev.3	Guide to Operational Technology (OT) Security	Sep 2023	NIST, U.S.	Yes / widely referenced
NIST SP 800-53 Rev.5	Security and Privacy Controls for Information Systems and Organizations	Sep 2020	NIST, U.S.	No / general IT controls
IEC 62645:2019	Nuclear Power Plants – I&C – Requirements for Security Programmes	Nov 2019	IEC, U.S.	Yes / nuclear specific
IAEA NSS 17-T Rev.1	Computer Security Techniques for Nuclear Facilities	2021	IAEA, International	Yes / nuclear specific
IAEA NSS 33-T	Computer Security of Instrumentation and Control Systems at Nuclear Facilities	2018	IAEA, International	Yes / nuclear specific
IAEA NSS 42-G	Computer Security for Nuclear Security	2021	IAEA, International	Yes / nuclear specific
IAEA NR-T-3.30	Computer Security Aspects of Design for I&C Systems at Nuclear Power Plants	2020	IAEA, International	No / tech guide for system designers, vendors
NRC RG 5.71 Rev.1	Cyber Security Programs for Nuclear Power Reactors	Feb 2023	U.S. NRC, U.S.	Yes / nuclear specific
NEI 08-09 Rev.7	Cyber Security Plan for Nuclear Power Reactors	Feb 2024	NEI, U.S.	Yes / nuclear specific
IEC 62859:2019	Requirements for Coordinating Safety and Cybersecurity	Oct 2019	IEC, International	No / paywalled, no access
IEC 62443 (series)	Security for Industrial Automation and Control Systems	2019-2024	IEC, International	No / paywalled, no access
ISO/IEC 27001:2022	Information Security Management Systems – Requirements	Oct 2022	ISO/IEC, International	Yes / widely referenced
ISO/IEC 27002:2022	Information Security Controls	Feb 2022	ISO/IEC, International	No / paywalled, no access
ISO/IEC 27019:2024	Information Security Controls for Energy Utility Industry	Oct 2024	ISO/IEC, International	No / paywalled, no access
ISO/IEC 27036-3:2023	Cybersecurity – Supplier Relationships – Part 3: ICT Supply Chain Security	Jun 2023	ISO/IEC, International	No / paywalled, no access
ISO/IEC 15408-1:2022	Evaluation Criteria for IT Security — Part 1: Introduction and General Model	Sep 2022	ISO/IEC, International	No / paywalled, no access
STUK YVL A.12	Information Security Management of a Nuclear Facility	Feb 2021	STUK, Finland	Yes / nuclear specific
CSA N290.7-14	Cyber Security for Nuclear Power Plants and Small Reactor Facilities	Jan 2021	CSA Group, Canada	No / paywalled, no access

Appendix 4 – Validation interview questionnaire

1. Contextual Alignment

1.1 From your perspective, do the evaluation criteria used in the thesis reflect Estonia's actual cybersecurity and institutional needs for the SMR program?

1.2 Do you see any important criteria missing that should be considered when evaluating CS standards and guidelines in this context?

2. Evaluation Results

2.1 Based on your experience, do the top-scoring standards (IEC 62645, IAEA NSS 17-T, STUK YVL A.12, ISO/IEC 27001) represent a suitable core for Estonia’s regulatory foundation?

2.2 Are there any gaps, limitations, or misjudgments in the scoring results or document selection that stand out to you?

3. Practical feasibility of recommendations

3.1 Are the proposed recommendations, particularly the phased implementation logic, realistic in Estonia's context (institutionally, legally, and politically)?

3.2 Do you agree that a hybrid framework approach (nuclear-specific + general cybersecurity governance) is appropriate for Estonia?

3.3 Are there any recommended actions or assumptions that you consider unfeasible or premature based on your understanding?

4. Institutional and legal considerations

4.1 What is your view on the thesis's observation that cybersecurity responsibilities are unclear in Estonia’s nuclear planning process?

4.2 Should nuclear cybersecurity oversight be placed in a new regulator or integrated into an existing agency?

5. Additional Insights

5.1 Are there any factors, risks, or constraints not reflected in the thesis that you believe should be highlighted?

5.2 Would you suggest any specific frameworks, tools, or case examples that Estonia should examine further?