
Chapter 1

# CYBER SECURITY REQUIREMENTS IN THE NORWEGIAN ENERGY SECTOR

Janne Hagen and Oyvind Toftegaard

**Abstract** This chapter discusses ongoing developments in cyber security regulations in the Norwegian energy sector through research and government-industry cooperation. The focus is on cyber security policies for Norwegian electric power supply entities at the strategic, tactical and operational levels. The chapter promotes the integration of regulatory requirements with traditional cyber security standards tailored to electric power supply entities and highlights how the integration contributes to effective cyber security governance and risk management.

**Keywords:** Cyber security regulations, Norway, energy sector, electric power supply

## 1. Introduction

Norway has a population of about 5.5 million people and land area of roughly 385,000 $km^2$. It has temperate coastal and continental subarctic climates that contribute to risks associated with floods, storms, landslides and avalanches. Extreme weather events and human threats following World War II and the Cold War have motivated continuous efforts at building a hydroelectric power system under state and municipal control that is resilient to various natural, technological and anthropogenic hazards.

Norwegian sector-specific contingency regulations have existed since 1948. The regulations include various security requirements, including redundancy and contingency planning. In 2003, the regulations were revised based on research conducted by the Norwegian Defense Research Establishment (FFI) [3, 4], which recommended mitigation measures to address the vulnerabilities of the electric power supply system. The new regulations provide a holistic security regime for electric power supply contingencies, and cover physical, personnel and organizational security,


Published by Springer Nature Switzerland AG 2022
J. Staggs and S. Shenoi (Eds.): Critical Infrastructure Protection XV, IFIP AICT 636, pp. 3–21, 2022.
https://doi.org/10.1007/978-3-030-93511-5_1

redundancy, maintenance capacity, restoration ability, information technology security and industrial control systems security. In 2014, three Norwegian electric power sector entities created KraftCERT, the first energy computer emergency response team (CERT) in Europe.

The Norwegian Water Resources and Energy Directorate (NVE) regulates security and contingency planning in the hydroelectric power supply and district heating (thermal energy) systems. The goal is to minimize the power outage risk in order to reduce adverse primary and secondary societal consequences. Due to the focus on security and contingency, the Norwegian power supply system is highly reliable and delivers 99.99% of the annual energy demand. The few power outages that occur are primarily due to natural hazards such as extreme weather events and, less frequently, technical failures.

Meanwhile, cyber security awareness has increased as a result of data breaches in the Norwegian Parliament [14], ransomware attacks on several Norwegian businesses and the SolarWinds and Microsoft Exchange attacks of 2021. Although cyber attacks have not caused power outages in Norway, the threat is growing. A recent report from Norway's Office of the Auditor General [4, 12] emphasizes the need for continuous improvements in cyber security.

This chapter discusses how NVE develops regulatory requirements pertaining to cyber security, how the regulatory requirements are transformed to corporate policies and procedures, and how compliance is controlled. It stresses the importance of a holistic approach that covers physical security, cyber security, redundancy, people and processes to create a cyber-resilient power supply infrastructure.

## 2. Norwegian Electric Power Sector

The Norwegian power grid is associated with the European Union through the European Economic Agreement and is part of the European electricity market. Among European countries, Norway generates the largest percentage of electricity from renewable sources and has the lowest power sector emissions. At the end of 2020, Norwegian electricity generation amounted to 153 TWh. The vast majority of the generation capacity is hydroelectric. Wind power accounts for approximately 10% of the generation capacity and dominates investments. District heating (thermal energy) amounts to 4%.

A special feature of the Norwegian hydroelectric power generation system is its high storage capacity – Norway has half of Europe's reservoir storage capacity. Furthermore, more than 75% of the Norwegian electric power generation capacity is flexible. Hydroelectric power gen-

eration can be rapidly increased or decreased on demand at low cost. Balancing power supply and demand is vital to achieving resilience; imbalances in power production and consumption can lead to outages. The need for flexibility is underscored by the growing share of intermittent generation technologies such as wind and solar power.

The Norwegian electric power generation system plays a key role in the "green shift" towards clean energy and low carbon dioxide emissions. NVE [16] projects that the complete electrification of the transportation sector – road, rail and ferries – will require about 20 TWh and will not be realized until at least 2050. There are no signs that the importance of electric power supply will decrease in the coming decades.

Norway's electric power generation system leverages about 1,000 water storage reservoirs located up in the mountains. The reservoirs are essentially energy batteries that are interconnected through rivers and tunnels. Tunnels and pipes connect the reservoirs to hydroelectric power generation plants located downstream in the valleys. The power plants transform kinetic energy from flowing water to electricity.

Electricity is stepped up to a high voltage level for transmission by transformer stations located outside the hydroelectric power generation plants. Transformer stations step down electricity to a lower voltage level before delivery to consumers. As of 2021, Norway had more than 1,600 hydroelectric power plants and over 50 wind farms. While hydroelectric power generation is adjusted easily, electricity generation in wind farms depends on wind velocity. Variations in wind velocity make it difficult to ramp up or ramp down electricity generation at wind farms to meet demand.

Electricity generation and consumption must be balanced continuously and the alternating current frequency must be kept at 50 Hz. Norway has overhead power line and direct current cable connections to neighboring countries. Electricity generated by Norwegian hydroelectric plants, which is easily adjusted based on demand, is traded in the European energy market via energy stock exchanges. The energy market plays an important role in balancing Norwegian domestic electric power generation and consumption. During emergency situations, Statnett, Norway's national transmission system operator can override market mechanisms to balance generation and consumption, preventing cascading problems and outages. In surplus situations, Norway exports electricity. In deficit situations, Norway imports electricity.

Information technology is essential to managing Norway's electric power supply system. Maximum and minimum water levels in reservoirs and rivers are monitored and managed by NVE to protect fish stocks and prevent flooding. Power generation entities optimize electric-

ity production according to market needs, constraints on water use, and generation and transmission capacity. Decisions are supported by industrial process control systems or supervisory control and data acquisition (SCADA) systems. Industrial control systems are also used to manage electricity transmission in the grid that crosses fjords, mountains and valleys. In addition to supervisory control and data acquisition systems, power generation entities and distribution system operators use commodity information technology products to support business operations. These myriad systems collectively constitute the digital infrastructure that enables the operation of Norway's complex electric power supply system.

Supply chain risk is an increasing concern because the vast majority of information technology products and applications are developed and distributed by transnational enterprises. Meanwhile, cyber attacks such as those on SolarWinds and Microsoft Exchange impact commodity information technology systems. When new vulnerabilities are recorded in the Common Vulnerabilities and Exposures (CVE) database [8], it is important to address them quickly. However, as demonstrated by the SolarWinds incident, a patch can be turned into a cyber weapon. The important point is that detection capability is effective at reducing risk. Immediately after the SolarWinds and Microsoft Exchange incidents were announced, KraftCERT broadcasted information about vulnerabilities and mitigation measures to Norwegian energy sector entities. As a result, the incidents did not impact the security of the Norwegian electric power supply.

The information technology and operational technology infrastructures in the electric power supply system can be protected by enforcing diversity, redundancy and defense-in-depth measures, along with contingency plans and recovery capabilities that enable normal operations to be established quickly after incidents. Additionally, various physical, personnel, technical and organizational measures are required to achieve resilience. These measures are included in the Norwegian contingency regulations for the electric power supply system.

Figure 1 shows the digital value chain of the Norwegian electric power supply system. The Norwegian power supply system has deployed new digital technologies in electricity generation, transmission and distribution. A prominent example in the transmission side is the positioning of sensors on power lines to collect physical parameters such as temperature and vibration data [5]. Meanwhile, advanced metering (smart meter) infrastructures have been constructed across the country to manage power distribution to customers.

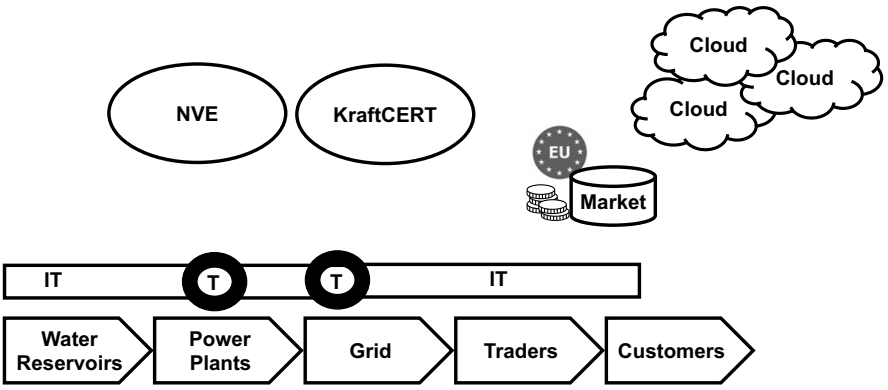


*Figure 1.* Digital value chain of the Norwegian elctric power supply system.

A study on innovation and the use of Internet of Things devices reports that several electric power sector entities intend to utilize sensors and data analytics for real-time control and effective operations and maintenance [15]. The study points to two trends. First, many projects are demonstrations, so large-scale implementations are still in the future. Second, vendors have expanded their services by offering innovative software solutions for data transmission, cloud services and data analytics, in addition to hardware. Extensive use of digital services and chains involving third parties increase system complexity and cyber security challenges. On one hand, they enable the electric power sector to apply innovative solutions to enhance operability and potential profits. On the other hand, the complexity and new dependencies induce latent, emergent risks.

## 3. Cyber Security Regulation Development

The Norwegian Ministry of Petroleum and Energy is responsible for energy policy. NVE's mandates are to ensure the integrated and environmentally-sound management of water resources, promote efficient energy markets and cost-effective energy systems, and contribute to efficient energy use. Also included are the responsibilities for national flood contingency planning and maintenance of the national electric power supply. NVE's Audit and Contingency Department oversees electric power infrastructure construction, security and contingency planning of water and energy facilities, technical energy installations and cyber security.

A 2015 report by the Norwegian Commission on Digital Vulnerabilities devoted an entire chapter to digital vulnerabilities in the electric

power sector [7]. However, in 2016, few cyber security incidents were registered by NVE, although electric power sector entities are required to report all extraordinary incidents. A subsequent NVE study of the cyber security status in the sector revealed that at least one-half of all entities had experienced Internet fraud and about 40% had detected computer viruses in their information technology systems [9].

In 2016, NVE established a project that sought to revise the contingency regulations on cyber security for the electric power supply sector. The project explored regulations in other industries and in other countries, regulatory regimes in the European Union and United States, and arranged workshops on cyber security and regulations for industry, government and other stakeholders.

NVE's final report recommended new regulations on traditional information technology systems. Industrial control systems were already well regulated; in fact, regulations inspired by the U.S. Federal Energy Regulatory Commission (FERC) [18] have existed since 2003 and they were revised extensively in 2013. The cyber security principles were generally regarded as valid, but they were continually being challenged by innovations in information technology and operational technology. It was clear that a new regulatory regime was required.

In 2018, NVE sought to formalize the cyber security regulations. The NVE team members had backgrounds in electrical engineering, cyber security and law. The team considered whether certification should be conducted based on international standards or statutory regulations. In Europe, the ISO/IEC 27001 standard is commonly used for information security management. While the efforts of a standardization committee comprising technical experts who attempt to comply with national regulations around the world are appreciated, certification according to an information security management standard only implies the existence of systems and procedures; it does not guarantee that security measures are implemented correctly. ISO/IEC 27001 also demands that entities perform risk assessments and choose appropriate security controls according to their levels of acceptable risk. Although this is good in principle, it does not enforce a minimum security level as in the case of compulsory regulatory requirements.

However, two advantages were discerned if NVE were to require certifications based on ISO/IEC 27001. First, NVE would not have to do audits, but instead collect certificates, check their validity and possibly sanction electric power supply entities with invalid certificates. The second advantage is that the information technology community would be familiar with the standards.

The NVE team produced two draft regulations. One draft was inspired by information security regulations in the Norwegian financial sector that build on the Control Objectives for Information Technologies (COBIT) framework [6]. The second draft drew from the efforts of the Norwegian National Security Authority (NSM), the responsible entity under the Norwegian Security Act, which has developed security baselines for Norwegian businesses based on *inter alia* international security standards. The Norwegian Energy Act and its contingency regulations cover various hazards, including natural, technological and intentional and unintentional anthropogenic hazards. However, the Norwegian Security Act, with its focus on intentional threats, does not apply to Norway's electric power supply sector.

Ultimately, the NVE team decided to base the cyber security regulatory requirements on the NSM baseline information technology security guidelines. The regulations do not explicitly mention the security baselines, but incorporate general security requirements that referred to international standards and norms. Nevertheless, the guidelines associated with the regulations link to NSM's baseline security requirements and other standards.

This approach provides an opportunity to leverage updated national baseline cyber security guidelines in the future. NVE released the revised regulations with the new requirements in an open hearing with a request for comments to be made within a few months. Minor changes to the regulations were made as a result of the hearing. Industry largely agreed that stricter regulation of information technology security were needed. The new regulations came into force on January 1, 2019.

## 4. New Cyber Security Contingency Regulations

The new Norwegian contingency regulations on cyber security cover requirements for securing information technology systems. According to the new regulations, entities shall:

- Secure digital systems to maintain confidentiality, integrity and availability
- Implement security measures
- Apply baseline security according to recognized standards and norms, including the following actions:
  - Identifying and documenting services and systems
  - Performing risk assessments
  - Securing systems and detecting security incidents

- Managing and restoring systems after attacks and failures
- Maintaining or increasing the security level when outsourcing tasks
- Performing security audits

Temporary guidelines followed the new regulatory requirements. On NVE's request, Energi Norge, an association of electric power supply entities, arranged to offer four courses on the regulations. Personnel from NVE, NSM, Norwegian University of Science and Technology (NTNU) and Elvia, Norway's largest distribution system operator, gave lectures on the new regulations and provided practical guidance on complying with the new requirements. NVE also arranged a seminar in Oslo that focused on the main changes in the new regulations. The seminar was well attended by Norwegian energy sector entities.

Changing regulations will not effect change on its own. It is vital to communicate the changes and disseminate information to industry entities. Familiarity with the new regulations is not enough. As discussed below, the intent of the regulations and their requirements must be understood and accepted by the stakeholders.

## 5. Development of Guidelines

In 2019, NVE established a working group and appointed a multidisciplinary team to revise the guidelines according to the new regulations. The coverage included cyber security, industrial control systems security, electrical engineering, risk management, emergency preparedness and legal issues. The effort had to balance the specificity of recommendations against the risk of becoming outdated and losing relevance in the long run. Guidelines that are frequently changed provide unstable frameworks, which are neither useful to industry nor the regulator to ensure compliance over time.

The final guidelines developed by NVE comprised eight chapters with one sub-chapter for each section in the regulations [11]. Each section presented the regulatory requirements, NVE's interpretation of the requirements and examples based on advice given to industry on the interpretations of the requirements. User-friendly "Attention!" and "Learn More!" boxes were incorporated. The "Learn More!" boxes provided links to international standards, guidelines and relevant reports produced by Norwegian authorities as well as foreign organizations like the U.S. National Institute of Standards and Technology (NIST). Standard symbols were used throughout the guidelines. Cross-references were provided to other sections in the regulations. The guidelines attempt to

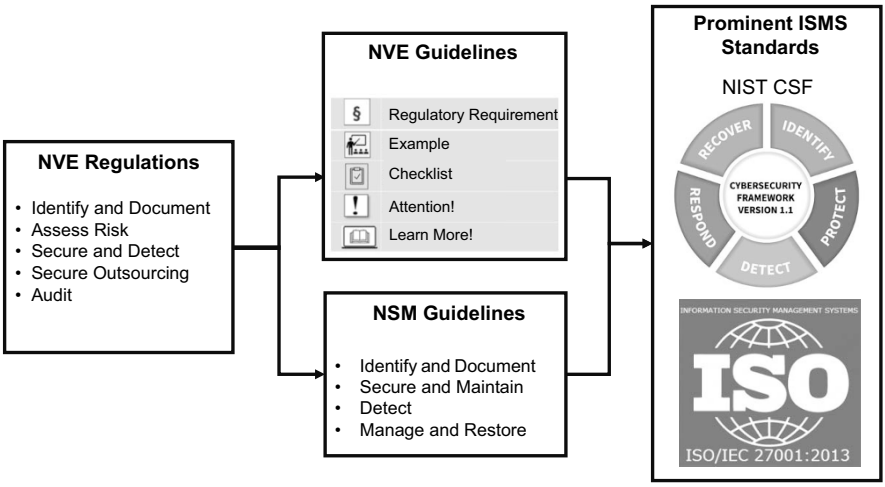


*Figure 2.* Alignment of NVE regulations with the NSM, NIST and ISO/IEC regimes.

communicate conflicts between standards, guidelines and statutory requirements. When conflicts occur, the statutory requirements always prevail.

The new guidelines were published in December 2020. In January 2021, a webinar was conducted to disseminate the guidelines to the stakeholders. Industry was given three months to study and comment on the guidelines. As it turned out, NVE received a few comments and minor changes were made to the guidelines.

## 6. Interoperability Principles

To ensure that cyber security regulations are timely, functional and relevant, NVE has attempted to make them compatible with other regulatory frameworks, guidelines and international security standards. Since entities in the energy sector may be subject to other regulations related to data privacy and national security imposed by the Norwegian Data Protection Authority and NSM, respectively, it is important that the NVE regulatory requirements and guidelines do not conflict with these and other requirements, as well as guidelines that would hinder compliance.

Figure 2 illustrates the alignment of the core content of NVE's contingency regulations with the NSM's security baseline guidelines and the prominent information security management standards. The security principles presented in the NSM guidelines are introduced as the first

step towards fulfilling the obligations of the Norwegian Security Act and its regulations. At this time, the Norwegian Security Act does not apply to power supply system entities. However, the NVE and NSM regulations both apply to critical community functions.

Interoperability of regulations, guidelines and standards provides two key advantages. First, entities that attempt to comply with NVE regulations and eventually the National Security Act can discern the common structure across the two regimes, rendering them easy to understand and implement. Second, organizations subject to NVE regulations may still use NSM security guidelines effectively to establish baseline security. Such crossover use is simplified because NVE regulations are carefully matched with NSM security principles. Close coordination between regulatory authorities is required to facilitate successful integration.

NSM security guidelines are also designed to dovetail with common information security management standards such as the U.S. National Institute of Standards and Technology Cyber Security Framework (NIST CSF) and ISO/IEC 27001 Information Security Management Standard (ISMS). As shown in Figure 2, the main principles of the NSM security guidelines are similar to the main principles of the NIST CSF framework. In addition, the NSM security guidelines are designed to enable entities to populate the guideline sub-categories with detailed security measures in the ISO/IEC 27001 ISMS standard. To assist entities that comply with the ISO/IEC 27001 ISMS standard, NSM has prepared a matching list that mirrors its guidelines and content in the ISO/IEC 27001 ISMS standard.

## 7. Cyber Security Policy Implementation

The understanding of the term policy varies between industry and academia. In this context, the term policy is a statement of objectives, rules, practices and/or regulations that governs the behavior of entities and/or the activities of individuals in a given context [13].

The distinction between public policies and corporate policies must be clarified. Public policies are systems of laws, regulatory measures, courses of action and funding priorities concerning topics promulgated by governmental entities or their representatives [2]. Regulatory requirements, such as laws, have a central role in public policy because they are often used to enforce policy compliance.

In contrast, corporate policies include strategies, rules, guidelines and procedures. It is common to divide corporate policies into three hierarchical levels, strategic, tactical and operational [19]. Strategic policies address corporate risks while complementing applicable laws; they

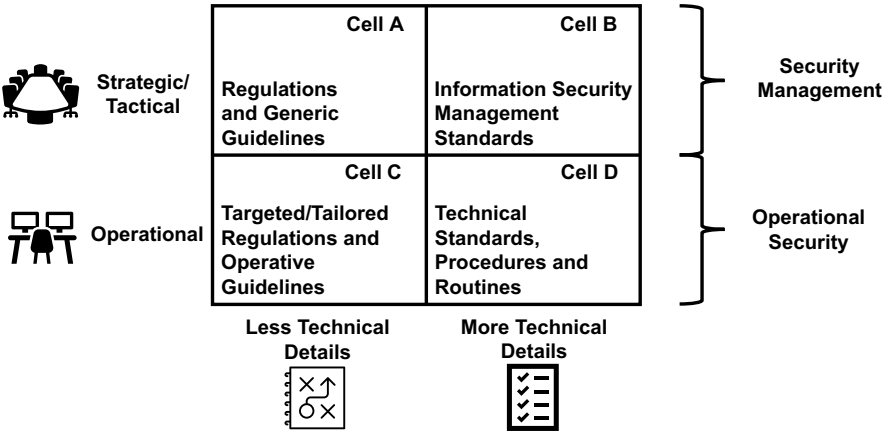


*Figure 3.* Relationships between public and private sector policies.

provide high level objectives with regard to security. Tactical policies include plans for extraordinary incidents such as contingency and crisis management plans, security maturity models, risk assessments, asset evaluations and information classification and other ways of guiding security implementations. Operational policies include routines and checklists for day-to-day monitoring and implementation of security requirements, such as permitting and revoking access rights, updating firewall rules, updating encryption protocols and installing security updates.

The level of detail is typically greater at the operational level and more generic at the strategic level. While the focus at the strategic level is on management and business processes, the focus at the operational level is on the technological aspects. Note that NVE does not regulate operational aspects such as the choice of information technology.

Figure 3 illustrates the relationships between public and private sector policies related to security management, operational security and level of technical detail. Regulations are in many cases generic and manifest long-term perspectives. Therefore, regulations are placed in Cell A, reflecting less technical detail at the managerial level. Crafting and approving regulatory requirements require considerable time and effort, and they should not be changed too often. Reducing the pace at which regulations are modified gives industry entities legal stability while they work on complying with the regulations. When requirements are specific and stipulate details, such as a specific technological solution, they may risk becoming obsolete and irrelevant.

Guidelines that specify generic activities also belong in Cell A. In this case, the effectiveness of security measures may be in focus. Examples are guidelines pertaining to asset management and risk assessment.

Asset management and risk assessment are also covered in the NIST CSF and ISO/IEC 27001 standards. Although these standards primarily specify management policies, they also cover technical security aspects in detail. Therefore, these standards are placed in Cell B in Figure 3. Organizations may utilize information security management standards to systematize their security regulation compliance efforts. NVE also requires organizations in the energy sector to implement security management systems.

Standards differ from regulations in that they are not intrinsically compulsory. NVE as a regulatory authority has little influence on the security controls from the various standards that Norwegian energy sector entities choose to implement. It is common for a standard such as ISO/IEC 27001 or NIST CSF to encourage entities to follow a risk-based approach and select controls from the standard that meet their risk assessment results and risk acceptance levels. However, NVE can enforce controls from standards through regulation. If NVE were to choose such a path, active participation in the standardization committees and their working groups could ensure some influence on the content of the requirements in the standards.

Although information security management standards may be detailed, they still reside at the managerial level and do not explain how the security measures should be implemented in practice. Therefore, entities may have to develop their own detailed procedures and routines or look to strictly technical standards such as IEC 62443 for industrial control system security or IEC 62351 for authentication. This is necessary to obtain the right level of detail for implementing the most technical requirements at the operational level. Cell D in Figure 3 contains the most technical and operational content that would support system operators in their daily security activities.

Tailored regulations and operative guidelines are placed in Cell C. These may be quite specific and feasible to follow at the operational level. However, as with other regulations and guidelines, they are made to last, and, therefore, do not discuss specific technological solutions. As an example, consider a hypothetical requirement that certain communications should be encrypted. Then, an entity with an information system that switches to encrypted communications on a mouse click could incorporate the requirement in an operational policy as a checklist entry. An entity without an information system with an encryption option would have to select an encryption standard in Cell D to implement

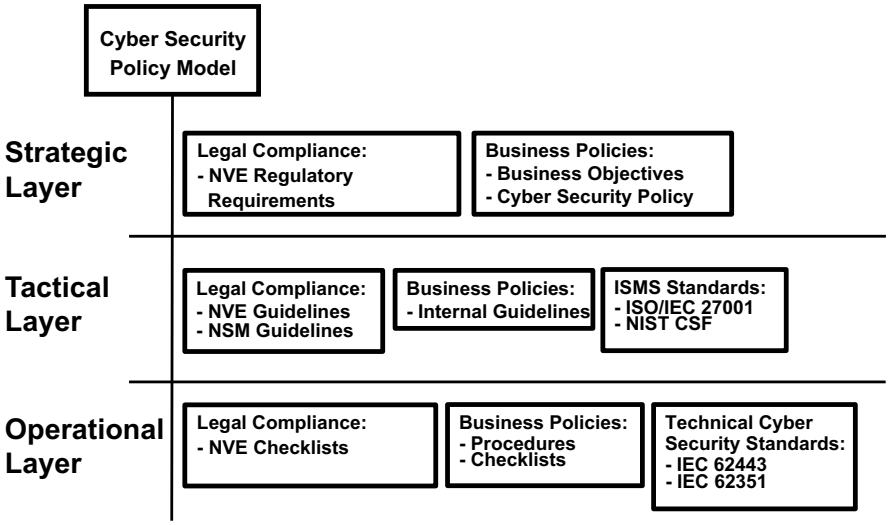


*Figure 4.* Hierarchical cyber security policy model.

the requirement. An advantage with this setup is that if the encryption standard chosen by the entity were to become obsolete, the tailored regulation or operative guideline in Cell C would still be relevant. Only the encryption standard in Cell D would have to be changed by the entity to satisfy the requirement.

## 8. Regulatory Requirement Compliance

Figure 4 shows a cyber security policy model with hierarchical layers of legal compliance, business policies and security standards. The policy model illustrates the principle of integration of regulatory requirements with traditional security standards tailored to the specific business roles of entities. The incorporation of cyber security regulatory requirements in business entity policies, supported by security standards where beneficial, may be key to successful and cost-effective security governance while ensuring legal compliance.

Norway has about 115 electric utilities. According to the European Union's definition of small enterprise [1], 88 Norwegian utilities would be small enterprises. Around 50 of these small utilities have less than 7,000 customers and struggle to have dedicated security staff. NVE has observed that some of these utilities comply with the minimum cyber security regulatory requirements and have minimal security governance. This often means that they merely have a general cyber security manage-

ment policy that addresses strategic security objectives, a cyber security handbook that addresses the regulatory requirements and a contingency plan. These small utilities have to follow the same regulatory baseline requirements as larger utilities. However, some regulatory requirements differ based on utility size. Specifically, systems and infrastructure assets are classified according to their size and importance. The greater the size and importance, the stricter the requirements.

NVE has observed that small utilities often outsource information technology services and operations. As a consequence, these entities often implement the security frameworks of their information technology service providers. The vast majority of these service providers have undergone thorough vetting prior to their engagements with larger utilities. As a result, they often have comprehensive security regimes that comply with the cyber security standards at the managerial and technical levels, boosting security management in the smaller utilities.

## 9. Audits

NVE oversees the effectiveness of cyber security governance in electric power supply entities via audits. Before the COVID-19 pandemic, NVE performed about 50 audits annually covering various parts of the contingency regulations. The major findings were related to risk assessment and contingency planning, but other issues were also identified by NVE during the audits.

An electric power supply entity is informed by mail about an impending audit. NVE requests documents related to the specific audit and the documents are thoroughly examined before the NVE site visit. The audit methodology uses standard checklists based on the sector regulations. NVE controls entity compliance using a selection of sections in the regulations. The audit is neither a certification nor a full revision nor a penetration test. During the daylong session involving discussions with and questions posed to electric power supply entity personnel, deviations from the selected sections of the statutory regulation are identified. A tradeoff exists between the level of detail to which NVE can investigate the security framework of a single entity and the number of entities that can be audited during a given period. At this time, the trend has been to audit more entities at lower levels of detail, inevitably hindering the identification of all possible deviations and vulnerabilities.

An NVE study has investigated the use of digital tools to improve the auditing process. For example, efficient auditing may be achieved by using open-source intelligence tools to monitor the release of sensitive information on the Internet [10]. This task could be performed by

the entities themselves after being trained in workshops or seminars, enabling NVE to enhance the quality and quantity of its audits. Scripts and vulnerability scanning tools would be employed to enhance the detection of technical vulnerabilities. However, such tools are not widely used by Norwegian authorities due to the potential negative impacts on the systems being evaluated [17].

NVE personnel would need to have the requisite technical skills to use digital tools in audits. If such skills do not exist in-house, NVE would have to hire a third-party for this purpose. This issue is being considered and a decision has yet to be made.

During its audits, NVE has mainly observed deviations related to risk assessments and their connections to contingency planning. There is also the potential for improving logging and log analytics for industrial control systems. NVE visits and audits have helped increase security awareness among top management that often participates in the meetings. Thus, the audits contribute to the creation of security cultures at the entities as well as increased investments in cyber security. Electric power supply entities are typically given three months to address issues identified in audits. Longer timeframes are given when large investments have to be made.

## 10. Potential Improvements

The Office of the Auditor General monitors the Norwegian public sector. In March 2021, the Office of the Auditor General [12] published a report about NVE's efforts in the energy sector. The report critiques the cyber security and contingency planning efforts and provides recommendations for improvement.

A key recommendation with regard to security governance is that NVE should improve the audit methodology. The report also recommends efforts focused on developing guidelines for the statutory requirements; this is important because statutory regulations currently do not apply to vendors with the exception of the requirements that protect sensitive information. Furthermore, the report highlights supply chain issues as a systemic risk. Supply chain security is regulated via private contracts between entities. NVE plans to explore ways in which its regulatory role may be leveraged to enhance supply chain security.

## 11. Conclusions

Developing prescriptive and flexible regulations that accommodate technological advances and organizational innovation is challenging. The impacts of technological advances and organizational innovation on secu-

rity should be investigated along with the relevance of current statutory requirements. NVE's experience reveals that small electric power supply entities prefer prescriptive regulations and highly specific advice whereas larger entities prefer functional regulations that give them the freedom to develop security policies and manage risk.

NVE's principal objective in regulating cyber security is to reduce the electric power outage risk and minimize adverse impacts on society. The Norwegian power supply system is highly reliable and delivers 99.99% of the country's annual electricity demand. Power outages in Norway are rare – they are primarily caused by extreme weather events and technical failures to a lesser degree. However, cyber security incidents are on the rise and demand increased attention and resources. As of 2021, cyber threats have been mitigated without any power outages. Nevertheless, this chapter argues that statutory regulations built on knowledge and international standards, with guidelines referring to standards, expert reports and subject matter expertise, can reduce the exposure to hidden and emergent risks associated with the digitalization of the electric power supply system. In addition, external audits are necessary to reveal deviations and improving auditing methods is a priority.

Successful governance requires an active regulator that conducts audits and sanctions electric power supply entities for non-compliance. This has contributed in part to the reliability of the electric power supply in Norway. Natural hazards are currently the dominant threats, but this will change as information technology increases its penetration in the electric power supply infrastructure. This is why updating regulations, guidelines and auditing methods in a timely manner, and communicating them to the various stakeholders are important. It is also important to keep abreast of advances in cyber security research and development and use the knowledge to update regulations and requirements. NVE looks to leading experts for advice and guidance, and has instituted partnerships with researchers from universities in Norway and the Nordic and Baltic countries, as well as in the United States to advance it energy regulation mission.

In conclusion, regulations are often viewed as hindrances by innovative business entities that seek to engage novel cyber technologies. However, it is prudent to carefully assess the current and emergent risks to the electric power supply system and implement security measures based on statutory requirements before going full speed ahead on the cyber highway.

## Acknowledgements

The authors wish to thank their colleagues at the Norwegian Water Resources and Energy Directorate, Head Engineer Helge Ulsberg and Head Engineer Amir Zaki Messiah, for providing valuable comments, and Ph.D. candidate Jenny Sjastad Hagen of the University of Bergen and the Bjerknes Center for Climate Research for her critical reading and language vetting.

## References

[1] European Commission, Internal market, industry, entrepreneurship and SMEs, Brussels, Belgium (ec.europa.eu/growth/smes/sme-definition_en), 2021.

[2] S. Evans (Ed.), *Public Policy Issues Research Trends*, Nova Science Publishers, Hauppauge, New York, 2008.

[3] H. Fridheim, J. Hagen and S. Henriksen, A Vulnerable Electrical Power Supply – Final Report from Protection of Society (BAS3) (in Norwegian), Norwegian Defense Research Establishment, FFI Report 2001/02381, Oslo, Norway (publications.ffi.no/nb/item/asset/dspace:3605/01-02381.pdf), 2001.

[4] J. Hagen, Securing the energy supply in Norway – Vulnerabilities and measures, presented at the *NATO Membership and the Challenges from Vulnerabilities of Modern Societies Workshop of the Norwegian Atlantic Committee and the Lithuanian Atlantic Treaty Association*, 2003.

[5] Heimdall Power, The power of knowing, Sandnes, Norway (heimdallpower.com), 2021.

[6] Information Systems Audit and Control Association, COBIT – An ISACA Framework, Schaumburg, Illinois (www.isaca.org/resources/cobit), 2021.

[7] O. Lysne, K. Beitland, J. Hagen, A. Holmgren, E. Lunde, K. Gjosteen, F. Manne, E. Jarbekk and S. Nystrom, Digital Vulnerabilities – Safe Society (in Norwegian), NOU 2015:13, Norwegian Government Security and Service Organization, Oslo, Norway (www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf), 2015.

[8] MITRE Corporation, Common Vulnerabilities and Exposures (CVE), Bedford, Massachusetts (cve.mitre.org), 2021.

[9] Norwegian Water Resources and Energy Directorate, The State of Information Security in the Power Supply Sector (in Norwegian), NVE Report no. 90-2017, Oslo, Norway (publikasjoner.nve.no/rapport/2017/rapport2017_90.pdf), 2017.

[10] Norwegian Water Resources and Energy Directorate, Method for Identifying Power Supply Sensitive Information on the Internet (in Norwegian), NVE Factsheet no. 11 09/2019, Oslo, Norway (publikasjoner.nve.no/faktaark/2019/faktaark2019_11.pdf), 2019.

[11] Norwegian Water Resources and Energy Directorate, Power Supply Contingency Regulations – Guidelines (in Norwegian), Oslo, Norway (www.nve.no/nytt-fra-nve/nyheter-tilsyn/rettleiar-til-kraftberedskapsforskrifta), 2020.

[12] Office of the Auditor General of Norway, The Office of the Auditor General of Norway's Study of NVE's Work with ICT-Security in the Power Supply Sector (in Norwegian), Document 3:7 (2020–2021), Oslo, Norway (www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen.pdf), 2021.

[13] A. Oldehoeft, Foundations of a Security Policy for Use of the National Research and Educational Network, NISTIR 4734, National Institute of Standards and Technology, Gaithersburg, Maryland, 1992.

[14] Reuters Staff, Norway's Parliament hit by new hack attack, *Reuters*, March 10, 2021.

[15] M. Royksund and A. Valdal, An Exploratory Study of the Application of Internet of Things (IoT/IIoT) in the Norwegian Power Supply Sector (in Norwegian), NVE External Report no. 2/2020, Norwegian Water Resources and Energy Directorate, Oslo, Norway (publikasjoner.nve.no/eksternrapport/2020/eksternrapport2020_02.pdf), 2020.

[16] D. Spilde and C. Skotland, How Could Extensive Electrification of the Transportation Sector Influence the Power Supply System? (in Norwegian), NVE Note, Norwegian Water Resources and Energy Directorate, Oslo, Norway (beta.nve.no/Media/4117/nve-notat-om-transport-og-kraftsystemet.pdf), 2015.

[17] T. Svensen, K. Kallseter and S. Husabo, Application of Digital Tools in ICT-Security Audits (in Norwegian), NVE Report no. 38/2020, Norwegian Water Resources and Energy Directorate, Oslo, Norway (publikasjoner.nve.no/rapport/2020/rapport2020_38.pdf), 2020.

[18] Technical Support Working Group, Securing Your SCADA and Industrial Control Systems, Version 1.0, U.S. Department of Homeland Security, Washington, DC, 2005.

[19] R. Wies, Policy definition and classification: Aspects, criteria and examples, *Proceedings of the IFIP/IEEE International Workshop on Distributed Systems: Operations and Management*, 1994.