A Checklist for Supply Chain Security for Critical Infrastructure Operators

Martin Gilje Jaatun[1] and Hanne Sæle[2]

[1] Department of Software Engineering, Safety and Security, SINTEF Digital, Trondheim, Norway
martin.g.jaatun@sintef.no
[2] SINTEF Energy, Trondheim, Norway
hanne.saele@gmail.com

Abstract. Critical infrastructure applications do not emerge fully formed, but generally rely on components and services from third-party vendors. This paper presents a brief survey on good practice for security requirements to be put on vendors delivering products and services to power Distribution System Operators and other critical infrastructure operators.

Keywords: supply chain, critical infrastructure, power distribution networks, security

1 Introduction

The objective of this work is to identify good practice on requirements related to ICT security in tender documents on procurement of Information Technology (IT) and Operational Technology (OT), and how this can be followed up in operation. An important result will be recommendations and/or good practices that can improve supply chain safety for small and medium-sized players, and we have taken this into account when assessing the summary of the selected articles.

This work has been performed in the context of Norwegian power Distribution System Operators (DSOs), but we believe that our recommendations to a large extent will be applicable to other critical infrastructure operators in Europe.

2 Method

We have reviewed and assessed recommendations from reports and academic literature that are relevant to the assignment. In the first instance, we have studied 3 reports (in Norwegian) commissioned by the Norwegian Water Resources and Energy Directorate (NVE):

- Elisabeth Kirkebø, Mathias Ljøsne, ICT security in procurement and outsourcing in the energy industry (in Norwegian), NVE Report 90:2018. [11]

– Maren Maal, Katrine Krogedal and Arthur Gjengstø, ICT security in procurement and outsourcing in the power industry - checklist (in Norwegian), NVE Report no. 1/2020 [13]
– Sigrid Haug Selnes, Sina Rebekka Moen, Siyang Emily Ji and Ove Njå, Power industry supply chains – digital security and vulnerability in the age of globalisation (in Norwegian), NVE-External Report 18:2021 [19]

The review of the reports from NVE described important topics related security, focused on the most relevant topics related to Supply Chain Security. NVE report 90:2018 [11] showed how dependent the energy business is related to their vendors, for example related to use of cloud services and outsourcing resulting in long digital value chains. The NVE report 1:2020 [13] is a checklist for procurement and outsourcing within the energy business, based on how increased digitalisation affect the risk picture for the business. The checklist is focusing on different phases such as preliminary phase, procurement, implementation and management, and termination. The third report (18:2021 [19]) describes a study of supply chain vulnerability and security, performed in the summer 2021, and based on interviews with relevant persons from the energy business, literature survey and questionnaires. The report gives recommendations related to how the energy business can understand digital vulnerability in the supply value chains, and how enterprises can work to reduce these vulnerabilities. Additionally, we have studied NVE's guide to the Norwegian Power Contingency Regulation [17].

Furthermore, we conducted a literature search in Scopus, as described in Section 3 below. In addition, we have conducted a small number of informal interviews with players in the power industry to obtain feedback on preliminary results and new input.

3 Literature search

We have used a simplified version of the guidelines for systematic literature analysis [12], where we first sort by title, then by abstract, and finally by the full text of the article. This is illustrated in Fig. 1.

Selnes et al. [19] performed a literature review on supply chain security in 2021. They provide examples of search strings, but it is not obvious how these are linked, as they state that ”The searches have resulted in a relatively small number of hits”. If we refine the search indicated in the offer to articles published after 2020, we get 322 hits, which is still too many for our purposes.

We therefore chose to refine the search to Selnes and colleagues. By searching Scopus with the criteria (”supply chain risk management” OR ”supplychain energy power supply” OR ”supply chain attack”) AND ”cybersecurity” AND (LIMIT-TO (PUBYEAR, 2022) OR LIMIT-TO (PUBYEAR , 2021)) we get 227 hits.

Scopus provides the ability to refine the search within subject areas. Through a spotcheck we found that if we narrow the search down to social science, business, and decision science, the results are largely irrelevant to our purpose, and by excluding these instead we come down to 119 hits:

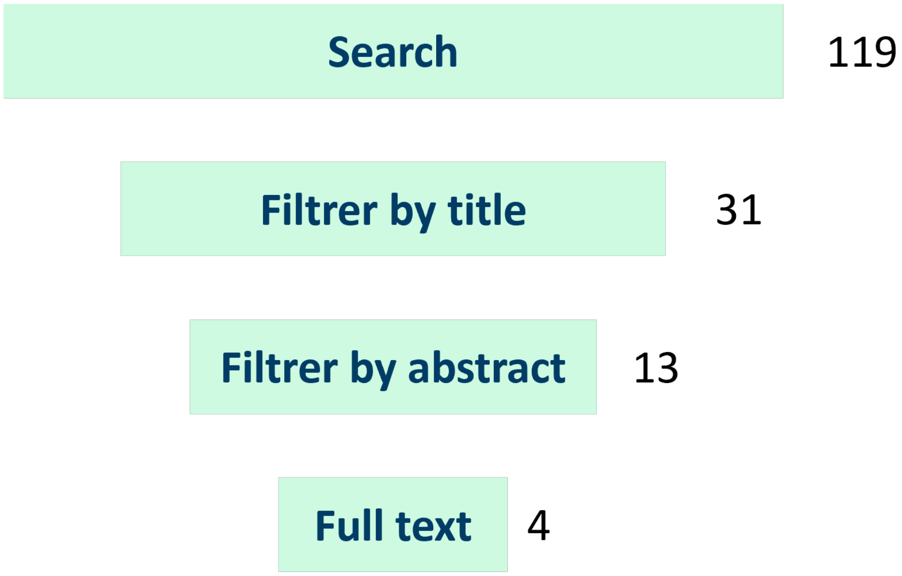

Fig. 1. Search strategy

> (”supply chain risk management” OR ”supplychain energy power supply” OR ”supply chain attack”) AND ”cybersecurity” AND (LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) AND (EXCLUDE (SUBJAREA , ”BUSI”) OR EXCLUDE (SUBJAREA , ”DECI”) OR EXCLUDE (SUBJAREA , ”SOCI”))

After reviewing all titles, the number of articles is reduced to 31 (see Appendix A for the full list). We have also excluded all articles dealing with the use of blockchains, as we do not consider this to be mature technology.

We then reviewed abstracts for the 31 articles.

3.1 Search Results

Among the 31 articles that were relevant based on title, we have considered 4 as relevant and a further 9 as possibly relevant to our work. Due to the limited time available, we have initially only looked into the 4 articles we initially considered to be relevant.

Struggling with Supply-Chain Security Viega and Michael [21] highlight that the most important supply chain security tool stands out as a standardized questionnaire/checklist for vendors, and point to the Vendor Security Alliance as a good example. They highlight that the wide range of service-based solutions represents a challenge for supply chain security.

They recommend using a risk rating of vendors, and then ensuring that those at greatest risk are reassessed at a higher frequency (e.g. annually). However, they point out that asking vendors for self-evaluation has significant challenges; They report on their own experiences where vendors have been caught lying about their security solutions. It motivates a desire for more automated solutions or monitoring of a vendor's solutions, in order to verify that the delivered security level harmonizes with the alleged security level. This may also include, for example, that the customer[3] can conduct monitoring of online forums where security leaks are shared, in order to detect security incidents before they are notified through official channels.

On the Feasibility of Detecting Software Supply Chain Attacks Wang [22] describes an experimental method for detecting supply chain attacks, but does not contribute anything that can be used to make demands on customers or vendors.

SoK: Combating threats in the digital supply chain Nygård and Katsikas [18] present a systematic review of literature with search terms: (Cybersecurity OR security) AND supply AND chain). Search results are further refined several times using keywords like ”attack” OR ”vulnerability” OR ”trojans” OR ”trust.”

The article mentions advice from NIST, but little that can be used to set requirements for vendors. One exception: ”Implement a documented vulnerability management program.”

SolarWinds Software Supply Chain Security: Better Protection with Enforced Policies and Technologies Yang, Lee and McDonald [23] describe a specific case, where the vendor SolarWinds who developed a popular management tool, Orion, was compromised by a group that accessed the source code of the product, and had a backdoor (known as SunBurst) added, which was then distributed by the provider as a valid update.

The authors discuss causes and consequences for SolarWinds and their customers, and identify a number of factors with proposed solutions. These are summarized in Table 1, with our comments.

The authors have additional recommendations on detecting vulnerabilities in open source dependencies, which is consistent with others' recommendations to use the Software Bill of Materials (SBOM) [14].

[3] Note that in this paper we use the term ”customer” to refer to the critical infrastructure operator who is buying goods or services from a vendor

Table 1. Problems identified by Yang, Lee and McDonald

Problem	**Proposed Solution**	**Our Comment**
The market focuses on profit, not security	– The government should set minimum security standards for software development and deployment – Improving the state's purchasing processes so that firms ensure security – Introduction of liability for software companies	Common guidelines may be beneficial, but we are sceptical whether introducing liability will have the desired effect – will be an expensive process, and in the end, large firms with many lawyers will be able to do as they please anyway.
"Additive" security adds new tools that potentially create new vulnerabilities	"Reductive" security that removes unnecessary services, libraries, etc.	This is in practice what is known as "hardening", and is something that can be recommended in general
Need to update to the next version	Refrain from updating if updating is unnecessary	Potentially a dangerous recommendation, as updates often correct detected security flaws
Customers rely on digitally signed updates	Create tools to easily assess the security of updates	Naïve approach that could cover this particular case, but in the general case, signed updates must be trusted. In the same way that today's antivirus tools are not 100% accurate, such a tool the authors recommend could not be.
Too much emphasis is placed on firewalls and antivirus and public cloud confidentiality requirements	– Use strong encryption everywhere – Move data stored in the cloud around	Here it seems that the authors do not know what they are talking about
Major challenge to carry out damage assessment and detection of modified components	Use AI to detect reconnaissance, command and control, and other signs of compromise	This is in practice a recommendation to use intrusion detection systems (IDS)

4 Recommendations for IT and OT procurement requirements, with a particular focus on supply chain

In the following, we will provide requirements for vendors, divided into "must-requirements" and further recommendations.

The requirements are assessed as "must" and "additional recommendations" based on the following criteria:

- Obligatory requirements: The requirements are based on requirements in current regulations (regulatory requirements). Please note, however, that we interpret this further than just NVE's area of authority, so that, for example, requirements that come from GDPR also apply here. Please also note that Section 6.9 of the Power Contingency Regulation [16, 17] lays down relatively broad guidelines for securing of digital information systems.
- Additional recommendations: Based on recommendations from a limited number of interviews with players in the power industry, recommendations from previous NVE reports, and recommendations from peer-reviewed literature in the last two years

The requirements as presented must be regarded as a first draft, and we recommend that a major "consultation round" be conducted with DSOs and vendors to obtain feedback before the NVE formalises the requirements. A critical infrastructure operator is free to upgrade "should" requirements to "must" requirements in a specific tender.

4.1 Prerequisites for DSOs

An important prerequisite for successful procurement of goods and services is to have sufficient procurement competence [5]. Procurement competence is a broad term, and includes general business competence, ICT security competence, integration competence, competence in procurement and legal competence. In order to make good orders, you need interdisciplinary expertise. According to NSM [5], business competence is needed to be able to define needs and set relevant requirements, and ICT security competence is therefore needed to be able to set reasonable security requirements. Knowledge of the business is also important in order to assess how what you order can be integrated into existing systems, and it is necessary to have knowledge of existing APIs, protocols and other interfaces. For example, if existing systems communicate with a given set of protocols, it can be disastrous if something is ordered that requires completely different protocols – we have seen several examples of this in recent times. General knowledge of procurement processes in the business is important to ensure that procurements fit into established patterns and routines (see also in the context of business understanding).

However, it is difficult to formulate universal requirements for this, and this is also difficult to measure. Large DSOs will typically have better access to ordering expertise than small DSOs. It will be important to collaborate between those responsible for the operation of IT/OT and the purchasing department. E.g., in connection with the roll-out of smart meters in Norway, many DSOs joined forces in alliances to meet the competence requirements in the procurement process.

4.2 Obligatory Requirements

The following requirements must be met by all power industry vendors.

Periodic risk assessment Vendors must be subject to periodic risk assessment so that DSOs can fulfil their duty protect their critical infrastructure [17]. The DSO can use checklists as described by Maal, Krogedal and Gjengstø [13].

Identify how vendors can assist in an emergency situation The vendor must document how it can assist the customer in an emergency situation involving the vendor's products or services, including incident management. This must be specified in the vendor contract or equivalent agreement.

Exercises Vendors must be involved in emergency preparedness exercises affecting their products and/or services [20], in accordance with what has been determined in section 4.2. This must be specified in the vendor contract or equivalent agreement.

This is not intended to be interpreted to mean that it should not be possible to arrange exercises without involving all vendors if the critical infrastructure operator considers it appropriate to also carry out more limited emergency preparedness exercises.

Location of servers If the service provided is to process sensitive information (personal data), the servers used by the service must be located in a country that satisfies the current rules for servers and personal data required by the GDPR law, which is currently EU/EEA [11][4]. This also applies to various forms of cloud solutions [2].

Power-sensitive information If the service provided is to process power-sensitive information (as defined in relevant regulations [16, 17]), servers used by the service must be located in a country that satisfies requirements for the procurement of operational control systems for classes 2 and higher.

[4] The GDPR does not strictly speaking require storing and processing of sensitive data within EU/EEA, but rather that such data can only be stored and processed in jurisdictions that have *sufficient protection*. However, with the Schrems II invalidation of the Privacy Shield agreement [8], it would be prudent to adopt a more conservative approach.

Location of employees If the service provided is to process sensitive information, the vendor's employees who gain access to such information must be physically located in the EU/EEA [11].

Beyond this requirement, vendors must also make additional assessments of nationality, depending on the type of tasks to be performed, even when there is no need for security clearance. Strategic/leading roles shall not be filled by employees with nationality from countries with which we do not have security policy cooperation.

Data ownership For services that involve the vendor processing the DSO's data in the vendor's infrastructure, it must be explicitly stated in the vendor contract that ownership of such data is retained by the grid company.

4.3 Additional recommendations

The following requirements should be met if possible, and justification should be given in cases where they are disregarded.

Software Bill of Materials All software should have a mechanism to trace the different parts of the software back to origin, and to keep track of which versions of software libraries etc. have been used, so that one can determine whether updating is necessary when new vulnerabilities are discovered. This can be in the form of a Software Bill of Materials (SBOM) [14] or equivalent solution. The vendor is responsible for maintaining an overview of the version that the customer is using at any given time, but this does not mean that the customer should have real-time insight into the details of the vendor's solution (e.g. in a SaaS solution). When a new vulnerability becomes publicly known, the provider should be able to immediately answer whether the service/product is affected by the vulnerability. This also means that the grid company should be able to monitor changes in products and/or services.

NSM basic principles or equivalent vendors should document the extent to which they satisfy NSM's Basic Principles for ICT Security [4] (level 1&2) or equivalent frameworks, such as ISO/IEC 27001 [10] or NIST CSF [15]. These two are examples of management standards/guidelines that have largely served as inspiration for NSM's basic principles. There are also more technology-oriented system standards such as IEC 62443 [9] that may be relevant.

VSA checklist New vendors should document their delivery in accordance with the Vendor Security Alliance (VSA) checklist [5]. The literature confirms that solutions such as questionnaires to vendors are among the primary tools used [21]. The checklist from the VSA is updated periodically.

[5] `https://www.vendorsecurityalliance.org/`

The checklist from VSA can be downloaded for free if you register on their website. There is an extended version and a kernel version, the latter consisting of a spreadsheet with 9 tabs:

- Introduction to the checklist
- Introduction to the service to be provided
- Data overview
- Security checks
- Introduction to privacy
- United States Privacy Policy
- GDPR privacy
- Definitions
- Legal terms

The data overview is used to clarify what types of data the provider collects from its users, e.g.:

- Age (presumably not relevant for a DSO)
- Address
- Education (presumably not relevant for a DSO)
- Email address
- ...

During security checks, there are questions such as:

- How do you encrypt [end user] customer data (in transit, at rest)?
- Which groups of employees (permanent and contracted) have access to personal and sensitive information about [end user] customers?
- Do you have a dedicated information security team? If so, how is it put together, and what report structure is in place?
- Do all personnel have to sign a non-disclosure agreement?
- How are regular updates evaluated for your infrastructure?
- Describe their incident management program.

Vulnerability management process The vendor should have a documented process for managing vulnerabilities in accordance with good practice, including a mechanism for deploying patches [6] [22].

Redundancy between subcontractors vendors should ensure redundancy so that alternative subcontractors can be used in the event of a loss of a subcontractor.

Transfer of data and configuration upon termination of contract The vendor contract should specify how the vendor will assist with the transfer of data and configuration to a new vendor upon termination of the contract.

Supply chain overview vendors should be able to document the complete (sub) supply chain of their product or service, especially across borders. NSM's recommendations on country assessment [3] (or similar guidance for other jurisdictions) should be taken into account when assessing the overall value chain.

Automated monitoring of services It will be beneficial if the provider can facilitate automated monitoring of the offered service to ensure that it meets the agreed security requirements at all times [21]. This may also include access to third-party audit reports. The DSO and/or relevant authorities should be able to perform audits.

Secure development It would be beneficial if the vendor could document a process for secure development in accordance with good practice [6, 7], e.g. as stated in IEC 62443 [1, 9]. The process must be appropriate for the product or service in question.

Hardening It will be beneficial if the products and services provided are "hardened" by removing all components and subsystems that are not strictly necessary [10].

Separation between customers It will be beneficial if the vendor can document how it ensures separation between customers, both technically and with regard to the extent to which personnel have access to data for several customers.

5 Conclusion and further work

This report presents results from a review of previous NVE reports on the topic of supply chain security, supplemented by a literature search among recent academic literature and discussions with a small selection of industry players, and recommends based on this a set of recommendations for requirements related to procurement of IT and OT, with a particular focus on supply chain.

Requirements and recommendations (must- and should-requirements) have been drawn up, aimed in particular at small and medium-sized grid companies for use in procurement processes. The requirements presented above must be regarded as a first draft, and we recommend that a major "consultation round" be conducted with DSOs companies and vendors to obtain feedback before the NVE formalises the requirements.

For more detailed requirements, more work should be done related to more empirical data and dialogue with different players in the industry – of different sizes. We see that there is a need for more coordination of procurement processes, and probably a consolidation must take place in the industry in the form of procurement alliances or the like in order to meet the challenges of making demands on the major vendors.

Requirements and recommendations should not only be based on historical experience, but also include assessments based on different scenarios and more proactive measures to ensure supply chain security.

Acknowledgements

This paper is based on research performed for the Norwegian Water Resources and Energy Directorate, expanded with support from the Research Council of Norway through FME CINELDI (project no. 257626) and SFI NORCICS (project no. 310105).

A Relevant papers based on title

Table 2 enumerates the papers that were identified as possibly relevant based on the title alone (listed in the order provided by Scopus). The final column reports the assessment of relevance after reading the abstract.

Table 2: Relevant paper titles

Nr	Title	Author(s)	Relevant?
1	Cyberattack Ontology: A Knowledge Representation for Cyber Supply Chain Security	Yeboah-Ofori, A., Ismail, U.M., Swidurski, T., Opoku-Boateng, F.	No
2	On the Feasibility of Detecting Software Supply Chain Attacks	Wang, X.	Yes [22]
3	Struggling with Supply-Chain Security	Viega, J., Michael, J.B.	Yes [21]
4	Information Security Assessment and Certification within Supply Chains	Santos, H., Oliveira, A., Soares, L., Satis, A., Santos, A.	No
5	SoK: Combating threats in the digital supply chain	Nygård, A.R., Katsikas, S.	Yes [18]
6	Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study	Martínez, J., Durán, J.M.	Maybe
7	Cybersecurity Certification Requirements for Supply Chain Services	Kyranoud, P., Kalogeraki, E.-M., Michota, A., Polemi, N.	Maybe
8	Economics of Supply Chain Cyberattacks	Kshetri, N.	No
9	Analytic hierarchy process (ahp) for supply chain 4.0 risks management	Zekhnini, K., Cherrafi, A., Bouhaddou, I., Benghabrit, Y.	Maybe
10	SolarWinds Software Supply Chain Security: Better Protection with Enforced Policies and Technologies	Yang, J., Lee, Y., McDonald, A.P.	Yes [23]
11	Risk Indicators and Data Analytics in Supply Chain Risk Monitoring	Stampe, L., Hellingrath, B.	No
12	IoT and Supply Chain Security	Kieras, T., Farooq, J., Zhu, Q.	No

Table 2: Relevant paper titles

Nr	Title	Author(s)	Relevant?
13	Applying NIST SP 800-161 in supply chain processes empowered by artificial intelligence	Al-Alawi, L., R. Al-Busaidi, and S. Ali.	No
14	Energy Resilience Impact of Supply Chain Network Disruption to Military Microgrids	Anuat, E., D.L. Van Bossuyt, and A. Pollman.	Maybe
15	Alice in (Software Supply) Chains: Risk Identification and Evaluation.	Benedetti, G., L. Verderame, and A. Merlo.	Maybe
16	Integrating Zero Trust in the Cyber Supply Chain Security	Do Amaral, T.M.S., and J.J.C. Gondim	Maybe
17	Cyber Supply Chain Risk Management and Performance in Industry 4.0 Era: Information System Security Practices in Malaysia	Fernando, Y., M.-L. Tseng, I.S. Wahyuni-Td, A.B.L. de Sousa Jabbour, C.J. Chiappetta Jabbour, and C. Foropon	Maybe
18	Supply Chain Flows and Stocks as Entry Points for Cyber-Risks	Filho, N.G., N. Rego, and J. Claro.	Maybe
19	Functional Requirements and Supply Chain Digitalization in Industry 4.0	Han, L., H. Hou, Z.M. Bi, J. Yang, and X. Zheng.	No
20	A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures	Hassija, V., V. Chamola, V. Gupta, S. Jain, and N. Guizani	No
21	I-SCRAM: A Framework for IoT Supply Chain Risk Analysis and Mitigation Decisions	Kieras, T., J. Farooq, and Q. Zhu.	Maybe
22	A Systematic Review of 2021 Microsoft Exchange Data Breach Exploiting Multiple Vulnerabilities	Pitney, A.M., S. Penrod, M. Foraker, and S. Bhunia	No
23	Internet of Things in Supply Chain Management: A Systematic Review Using the Paradigm Funnel Approach	Rajabzadeh, M., S. Elahi, A. Hasanzadeh, and M. Mehraeen.	No

Table 2: Relevant paper titles

Nr	Title	Author(s)	Relevant?
24	A Taxonomy for Threat Actors' Delivery Techniques	Villalón-Huerta, A., I. Ripoll-Ripoll, and H. Marco-Gisbert	No
25	A Data Processing Pipeline for Cyber-Physical Risk Assessments of Municipal Supply Chains	Weaver, G.A.	No
26	Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security	Yeboah-Ofori, A., S. Islam, S.W. Lee, Z.U. Shamszaman, K. Muhammad, M. Altaf, and M.S. Al-Rakhami.	No
27	Supply Chain 4.0 Risk Management: Bibliometric Analysis and a Proposed Framework	Zekhnini, K., A. Cherrafi, I. Bouhaddou, and Y. Benghabrit	No
28	On the Impact of Security Vulnerabilities in the Npm and RubyGems Dependency Networks	Zerouali, A., T. Mens, A. Decan, and C. De Roover	No
29	Cyber-Security Risk Management and Control of Electric Power Enterprise Key Information Infrastructure	Zhang, G., Y. Xu, Y. Hou, L. Cui, and Q. Wang.	No
30	Summary of Risk Warning of Electric Power Material Supply Chain	Zhang, Z., S. Feng, and T. Hu.	No
31	Evaluation Indicators for Open-Source Software: A Review	Zhao, Y., R. Liang, X. Chen, and J. Zou.	No

References

1. IEC 62443-2-4:2015 | Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers (2015), https://webstore.iec.ch/publication/22810
2. Cybersecurity — Supplier relationships — Part 4: Guidelines for security of cloud services (2016), https://www.iso.org/standard/59689.html, last reviewed in 2022

3. Anbefaling om landvurdering ved tjenesteutsetting - Nasjonal sikkerhetsmyndighet (Sep 2020), https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/anbefaling-om-landvurdering-ved-tjenesteutsetting/
4. Grunnprinsipper for IKT-sikkerhet 2.0 (Jun 2020), https://nsm.no/getfile.php/133735-1592917067/NSM/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf
5. Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester (Jul 2020), https://nsm.no/getfile.php/133998-1593590999/NSM/Filer/Dokumenter/Rapporter/2020-07-01%20-%20Temarapport%20-%20Tjenesteutsetting.pdf
6. Threat Landscape for Supply Chain Attacks. Report/Study (Jul 2021), https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
7. CISA: Defending Against Software Supply Chain Attacks (Apr 2021), \url{https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf}
8. European Parliament: The CJEU judgment in the Schrems II case, https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf
9. IEC: Understanding IEC 62443. IEC Blog (2021), https://www.iec.ch/blog/understanding-iec-62443
10. ISO: Information technology – security techniques – information security management systems – requirements. ISO/IEC Standard 27001:2013 (2013), https://www.iso.org/standard/54534.html
11. Kirkebø, E., Ljøsne, M.: IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen. Tech. Rep. Nr. 90/2018, NVE (Oct 2018), https://publikasjoner.nve.no/rapport/2018/rapport2018_90.pdf
12. Kitchenham, B.A.: Systematic review in software engineering: where we are and where we should be going. In: Proceedings of the 2nd international workshop on Evidential assessment of software technologies. pp. 1–2 (2012)
13. Maal, M., Krogedal, K., Gjengstø, A.: IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen - sjekkliste. Tech. Rep. Nr. 1/2020, NVE (Jan 2020), https://publikasjoner.nve.no/rapport/2020/rapport2020_01.pdf
14. Muirí, E.O.: Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM) (Nov 2019), https://ntia.gov/files/ntia/publications/framingsbom_20191112.pdf
15. NIST: Framework for improving critical infrastructure cybersecurity (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
16. NVE: Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften) (Jan 2019), https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157
17. NVE: Veiledning til kraftberedskapsforskriften (2022), https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/veiledning-til-kraftberedskapsforskriften/
18. Nygård, A., Katsikas, S.: SoK: Combating threats in the digital supply chain. In: Proceedings of the 17th International Conference on Availability, Reliability and Security. ACM International Conference Proceeding Series, Vienna, Austria (2022)
19. Selnes, S.H., Moen, S.R., Ji, S.E., Njå, O.: Kraftbransjens leverandørkjeder – digital sikkerhet og sårbarhet i globaliseringens tidsalder. Tech. Rep. 2021:18, NVE (2021), https://publikasjoner.nve.no/eksternrapport/2021/eksternrapport2021_18.pdf

20. Tøien, F.K., Fagermyr, J., Treider, G., Remvang, H.: IKT-sikkerhetstilstanden i kraftforsyningen 2021. Tech. Rep. Nr. 19/2021, NVE (2021), https://publikasjoner.nve.no/eksternrapport/2021/eksternrapport2021_19.pdf
21. Viega, J., Michael, J.: Struggling with Supply-Chain Security. Computer 54(7), 98–104 (2021), https://www.scopus.com/inward/record.uri?eid=2-s2.0-85112675156&doi=10.1109%2fMC.2021.3075412&partnerID=40&md5=9891b633e2cc6d2fcb9595acbfad99ac
22. Wang, X.: On the Feasibility of Detecting Software Supply Chain Attacks. vol. 2021-November, pp. 458–463 (2021)
23. Yang, J., Lee, Y., McDonald, A.: SolarWinds Software Supply Chain Security: Better Protection with Enforced Policies and Technologies. Studies in Computational Intelligence, vol. 1012 SCI. Springer (2022), pages: 58