Software Bill of Materials in Critical Infrastructure

Lars Andreassen Jaatun*, Silje Marie Sørlien*,
Ravishankar Borgaonkar†, Steve Taylor‡ and Martin Gilje Jaatun†§
*NTNU, Trondheim, Norway
†SINTEF Digital, Trondheim, Norway
‡University of Southampton, UK
§University of Stavanger, Norway

***Abstract*—Critical infrastructure today is comprised of cyber-physical systems, and therefore also vulnerable to cyber threats. Many of these threats come from within, through malicious code in software updates or bugs that can be exploited. Further exacerbating the issue is the fact that most software suppliers in critical infrastructure are developing proprietary systems and giving out minimal information about the composition of their software products. With the US introduction of a Software Bill of Materials (SBOM) requirement in federal information systems, they are better prepared to deal with cyber incidents. This article examines regulations regarding software in critical infrastructure, and whether there is any benefit to mandating SBOMs in critical infrastructure.**

***Index Terms*—SBOM, Critical Commmunication, Cyber Security, Software Security.**

I. Introduction

In 2021, the Linux Foundation conducted a survey which stated that 98% of the participants belonged to organizations that in one way or another used Open Source components in their products [1]. Using open source components instead of writing original code can speed up development, however more time should be spent on making sure components are up to date and to monitor vulnerability databases for any new relevant publicly disclosed vulnerabilities.

Today, there are several tools and services whose purpose is to help monitor potential vulnerabilities linked to such components. These tools scan source code and generate an overview of dependencies, vulnerabilities and suggestions for mitigation where possible. They can also monitor vulnerability databases and give notice if new vulnerabilities are linked to the dependencies in the project. These services are suitable for development teams, both during the development phase and after deployment. But this information is unavailable to users without access to the source code. To contribute to greater transparency around the content of software, "the Software Bill of Materials" (SBOM) has been developed.

A. Critical Infrastructure

Cyber warfare is becoming ubiquitous and critical infrastructure is often targeted [2]. Downtime in critical infrastructure may result in considerable loss of profit as well as physical damages. The software supply chain is a commonly used attack surface [3], and it is difficult to protect due to a lack of transparency in commercial products. A step towards better security in critical infrastructure is to improve communication of risks between suppliers and customers [4].

In light of recent cyber attacks on critical functions in Norway, and a subsequent need to strengthen cyber security in Norwegian organisations, it is very relevant to investigate how to monitor indirect vulnerabilities in critical software applications. After an inconclusive Google search on SBOM and Norway, we became interested in investigating this further and assessing the potential for introducing this as a standard in Norwegian-produced software and as a requirement for software applications adopted in Norwegian critical infrastructure.

Ensuring software transparency is attractive to buyers of software and is therefore a good marketing decision. It can also contribute to reduce costs by minimizing mitigation time and damage during down time. In the critical infrastructure domain, however, the risks to societal functions are far greater than damage to reputation or economic penalties. The Norwegian government defines the Norwegian critical infrastructure as 14 functions: Governance/information, power supply, oil and fuel supply, transportation, work force, banking and monetary system, construction, industry and trade, health, nutrition, fire and rescue, police and order, water supply and telecommunication [5]. Each of these functions are vulnerable to severe consequences in case of failure in or breach of the software they use.

B. The SBOM

An SBOM is a standardized list of components, modules and libraries used in a project, to ensure transparency about dependencies in software where the source code is not available to users [6]. This list can be used to check the dependencies against vulnerability databases, for example by using a service like Snyk or a tool like OWASP's dependency-check. An important function of SBOM is identifying nested dependencies and displaying them in dependency trees. There are currently (at least) three competing SBOM formats; SPDX from the Linux Foundation, CycloneDX from OWASP, and SWID as defined in

ISO/IEC 19770-2 [7]. Table 1 shows National Telecommunications and Information Administration (NTIA's) proposal for minimum requirements for the content of an SBOM.

In this literature review, we will research the potential benefits of introducing SBOM in critical infrastructure versus the risks of not using SBOM,and the advantages and disadvantages of introducing SBOM into ICT laws and regulations.

II. Research method

A search for "software bill of materials" and "critical infrastructure" in Google Scholar retrieved 75 results. To filter out irrelevant search results, we read the title and abstract of all results. We also considered papers in English only, ruling out an additional 4 papers. This left us with 37 sources that we believe are relevant for this article[1]. Out of these 37 papers, 15 mentioned SBOM once, 15 mentioned SBOM a few times and 7 mentioned SBOM several times. In addition to these articles, we searched Norwegian laws and guidelines to form a picture of the current regulations of software used in critical infrastructure in Norway. We have also done research on the executive order from the USA government administration on the use of SBOM in federal agencies [8].

As mentioned in the introduction, the Norwegian critical infrastructure is defined as 14 functions. Out of these 14 functions, we believe 4 of them has ICT as a main part; health, banking and monetary system, power supply and communication.

III. National laws and guidelines for software transparency

In January of 2019, the Norwegian National Security Authority (NSM) published a list of measures to be taken to improve national cyber security: *"Measures for the national strategy for digital security"*. This list contains plans to improve competence in the cyber security industry in Norway and plans to improve cyber security in general in all parts of the Norwegian critical infrastructure. The document is divided into *"Key measures for increased digital security"* and *"Optional measures for improved self-sufficiency"*. In the second part, NSM states that organizations should adhere to the basic principles for ICT security [9], where one sub-chapter is dedicated to *"Mapping out hardware and software"*. In these guidelines, NSM also states that organizations should maintain an overview of the software in use, preferably using an automated solution for quick vulnerability feedback, but nowhere in the guidelines is SBOM mentioned.

The NIS directive is an EU-wide piece of cybersecurity legislation that was approved in 2016. EU member states have since the approval of the legislation worked on integrating the directive into national laws [10]. The directive is awaiting approval from all member states of the EEA before official adoption in Norway, but the process of integrating the directive with Norwegian laws has already begun [11]. The NIS-directive sets requirements for security and incident response as well as standardisation across nations for better cooperation [12].

[1]Due to space limitation, we are not able to document all the literature in this paper, but we have provided a separate document here: http://sislab.no/lars/sbom-sources.pdf

IV. Software Bill of Materials in banking and monetary system

The Norwegian banking and monetary system is highly reliant on strong information security as it deals with sensitive data and crucial processes. The laws and regulations for this sector of the Norwegian critical infrastructure is governed by the Norwegian Department of Finance, the Norwegian Financial Supervisory Authority and Bank of Norway. In 2000, The emergency committee for financial infrastructure was established. Their responsibility is to assess risk, vulnerability and stability in the banking and monetary system in Norway [13].

"In the follow-up of ICT incidents in companies, Finanstilsynet emphasizes that causes are uncovered and measures are taken to prevent repetitions. Finanstilsynet is designated as the sector-specific response environment (SRM) in the financial market area in accordance with the National Security Authority's (NSM) framework for handling ICT security incidents. The supervisory authority exercises its role in collaboration with Nordic Financial CERT. Nordic Financial CERT has been established by Finans Norge to assist financial institutions in dealing with digital attacks. Nordic Financial CERT is from 2017 a Nordic organization with headquarters in Oslo." [14].

V. Software Bill of Materials in power supply

The electric power sector is an attractive target for malicious actors because of the ramifications of downtime in the grid on critical infrastructure. As the power sector depends more on IoT-sensors and new technology, the attack surface will increase.

Livingston et al. [15] wrote about cyber security in the power sector emphasising the importance of further developing security measures to counter new threats. The article states that supply chain attacks are more and more common, and is the primary cause of multiple large-scale attacks. An example mentioned in the article is notPetya, a virus injected into a software update that caused damages worth 10 billion US dollars. The article [15] refers to study of power and gas companies in North America stating that companies had on average 3647 active suppliers, of which few/none were monitored or questioned about their security practices.

The same article maintains that power grid companies located in the US are adopting SBOMs as a countermeasure against supply chain attacks [15]. A report by The MITRE Center for Technology & National Security [2] states that; *"... good industry practices increasingly mandate the use of an SBOM that identifies the provenance of the various components. If done properly, an SBOM can estimate the overall risk of the ensemble of software elements based on the risk of the individual elements. "*.

TABLE I
Different SBOM formats

NTIA SBOM Minimum Fields	**SPDX**	**SWID**	**CycloneDX**
Supplier Name	(3.5) PackageSupplier:	<Entity> @role (softwareCreator/publisher), @name	Publisher
Component Name	(3.1) PackageName:	<softwareIdentity> @name	Name
Unique Identifier	(3.2) SPDXID:	<softwareIdentity> @tagID	bom/serialNumber and component/bom-ref
Version String	(3.3) PackageVersion:	<softwareIdentity> @version	version
Component Hash	(3.10) PackageChecksum:	<Payload>/../<File> @[hash-algorithm]:hash	hash
Relationship	(7.1) Relationship: CONTAINS	<Link> @rel, @href	(Nested assembly/subassembly and/or dependency graphs)
Author Name	(2.8) Creator:	<Entity> @role (tagCreator), @name	bom-descriptor/manufacture/contact

The power grid in Norway is governed by the "Regulation on Safety and Preparedness". The document gives an in-depth description of how companies in the power sector should operate to maintain proper safety and contingency procedures, with a section dedicated to ICT. The most important guidelines cover identification and documentation of services, systems and other assets, risk assessment, discovering and mitigating threats, handling and recovering from attacks, and guidelines for outsourcing and safety revision. Importantly, the document states *what* should be done, but not *how*. [16]

VI. Software Bill of Materials in health

Carmody et al. [17] discuss the importance of resilience in medical technology and using SBOM to strengthen cyber security in healthcare. They state; *"SBOMs have the potential to benefit all supply chain stakeholders of medical technologies without significantly increasing software production costs. Increasing transparency unlocks and enables trustworthy, resilient, and safer healthcare technologies for all."* They proceed to mention benefits for buyers; *"For buyers, an SBOM helps evaluate risk at the time of purchase of a builder's product (e.g., when an healthcare delivery organizations buys a medical device from a medical device manufacturer)."*[17], regulators; *"For regulators, SBOMs provide a map of overall public health risk when a vulnerability is reported."*[17] and operators; *"For organizations and individuals who operate and maintain software, tracking an SBOM throughout the product's lifecycle allows a more proactive security posture by enabling operators to address newly discovered vulnerabilities before adversaries have a chance to compromise them."*[17].

The Medical Device Cybersecurity Working Group wrote an article to *"provide general principles and best practices to facilitate international regulatory convergence on medical device cybersecurity"* [18]. In this article, they identify cyber security as a shared responsibility between all stakeholders in medical device development. The authors state that better information sharing will lead to decreased risk in the supply chain and that for more effective information sharing, transparency in development is important. The article concludes that providing SBOMs throughout the supply chain can aid in creating more transparency, as well improving information exchange [18].

In 2014, the Norwegian government announced the Health Register Act with the purpose of ensuring safer collection and storage of health related data. It determines access control and the rights an individual has to change or remove data stored in the health registry. Paragraph 21 discusses information security and assigns the party responsible for data storage and processing the task of performing necessary measures to ensure a sufficient level of security [19]. Paragraph 21 does not explicitly describe the measures parties responsible for data processing and storage has to make to ensure information security. Therefore one can argue that it simply counts this party responsible for countering new threats to the database. This must be done by keeping up on new methods of securing data, processes and systems.

Carmody et al. [17] mention a plausible explanation for why the implementation of SBOM in the healthcare industry has been slow, citing *"a lack of out-of-the-box solutions and industry-wide standards"* resulting in organizations developing their own solutios independently. FOSSA [1] also comment on this concern, highlighting shortcomings when it comes to fixed frameworks around format, frequency of re-generation and depth of dependency trees. Some of this can be explained by the fact that SBOM is still relatively new.

VII. Software Bill of Materials in communication

Providers of critical communication services are subject to laws regarding safety and preparedness of electronic services and networks in Norway [20]. Two laws are the The Electronic Communications Act and the The National Security Act.

The Electronic Communications Act (Ekomloven) is summarized as; *"The purpose of the Act is to ensure users throughout the country good, affordable and forward-looking electronic communication services, through efficient use of public resources by facilitating sustainable competition, as well as stimulating business development and innovation."*[21]. Paragraph 2 to 10 describes the providers responsibility to ensure the safety and security of their

services and networks as well as their responsibility to maintain the necessary preparedness [22].

Some providers, including providers of critical services, are obliged to follow The National Security Act (Security Act). The Security Act is summarized as; *"The Act shall contribute to: a. securing Norway's sovereignty, territorial integrity and democratic form of government and other national security interests, b. preventing, uncovering and countering security-threatening activities, c. that security measures are carried out in accordance with basic legal principles and values in a democratic society."* [23].

In the National communication authority's annual report, they outline the steps they have been taking to improve information security in the past year [24]. In an effort to improve cyber security across multiple industries, NKOM has established a group consisting of companies from both the power and communication sector such as NVE and Telenor. The goal for establishing this group is to increase information sharing and communication between different companies nationally. Additionally, NKOM has been hard at work to ensure that communication providers are following the guidelines defined in the security law.

VIII. Software transparency by law

In 2021, the US government issued a presidential order that all federal agencies are obligated to follow, applicable to software deployed in the United States; *"... Such guidance shall include standards, procedures, or criteria regarding: ... (vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;"*. Furthermore, they specified; *"Within 60 days of the date of this order, the Secretary of Commerce, in coordination with the Assistant Secretary for Communications and Information and the Administrator of the National Telecommunications and Information Administration, shall publish minimum elements for an SBOM."* [8]. This suggests that there will be minimum requirements for what an SBOM should contain in the USA. The survey showed that the participants were missing a standard, so this could be the start of an industry-wide standard for SBOM.

In the same survey carried out by The Linux Foundation, the participants respond that they feel that SBOM has advantages that go beyond making it easier to monitor vulnerabilities linked to the components of the application. SBOM can also contribute to increased awareness and understanding of risks linked to the dependencies in a project and the importance of having control over vulnerabilities also outside the development team [1]. FOSSA summarizes the survey with 6 points [1]:

- "the presidential order has had an effect"
- more solutions are needed
- there are more benefits from SBOM than just security
- it's early days yet
- the most important needs are machine readability and dependency depth
- open source is ubiquitous

IX. Risk Modelling & SBOMs

Several citations above (e.g., Nissen et al. [2], Carmody et al. [17]) suggest that SBOMs are useful for determining risk, but do not state how. This section aims to address this question via mapping established risk management concepts to SBOMs, to show how SBOMs fit in with risk management.

Key concepts in risk management are defined in numerous sources, but given that this paper concerns software and its security, it is appropriate to focus in on Information Security risk management concepts, and popular sources of definitions in this subdomain are to be found in ISO 27000 [25] and RFC 4949 [26], so these will serve as the basis for definitions of the key concepts. These will be supplemented as necessary by ISO 27005, which describes an approach for Information Security risk management and ISO 14971 [27], which describes risk management for the subdomain of healthcare (specifically medical devices).

Asset "*A system resource that is (a) required to be protected by an information system's security policy, (b) intended to be protected by a countermeasure, or (c) required for a system's mission*" [26]. "*An asset is anything that has value to the organization and which, therefore, requires protection. For the identification of assets, it should be borne in mind that an information system consists of more than hardware and software*" [28].

Consequence "*Outcome of an event affecting objectives*" [28]. Also Harm: "*injury or damage to the health of people, or damage to property or the environment*" [27]. Also, Threat Consequence: "*A security violation that results from a threat action*" [26]. Consequence is the conjunction of the impact and the likelihood of the events that cause the consequence.

Control "*Measure that is modifying risk*" [25]. Also, Security Control: "*The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information*" [26].

Impact: from Consequence Criteria "*Consequence criteria should be developed and specified in terms of the extent of damage or loss, or harm to an organization or individual resulting from the loss of confidentiality, integrity and availability of information. [...] Consequence criteria define how an organization categorizes the significance of potential information security events to the organization.*" [28]

Likelihood: "*Chance of something happening*". [25]

Risk "*Effect of uncertainty on objectives*" [25]. Also Risk Level (Level of Risk) "*magnitude of a risk expressed in terms of the combination of consequences and their likelihood*" [25]

System: defined as Information System "*set of applications, services, information technology assets, or other information-handling components*" [25].

Threat "*potential cause of an unwanted incident, which can result in harm to a system or organization*" [25]. Actual manifestation of Threat is Information Security Event "*identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that can be security relevant*" [25]

Vulnerability "*Weakness of an asset or control that can be exploited by one or more threats*" [25]. The term 'vulnerability' is sometimes used to mean 'software vulnerabilities' (a specific type of vulnerability), and sometimes to mean 'threats to a system for which there are no controls' (a restriction based on vulnerability status). ISO 27000 does not include either of these restrictions and our interpretation of vulnerability can apply to any systemic asset including ICT hardware, computer software, networking, places, people and governance to reflect weaknesses that may increase the likelihood of their being affected by threats.

Beginning from the System and working anti-clockwise in Fig. 1, the key properties that determine the cause and effect of Threats on Risks are as follows.

- The System under examination is a cyber-physical system of different types of Assets and their relationships. As noted by ISO 270005, Assets are more than software artefacts, but this paper is concerned with SBOMs in Software Assets, hence the specific subclass of Software Asset inheriting from a generic Asset.
- Assets have Vulnerabilities that describe weaknesses. Here is the link to SBOMs - the SBOMs can inform on the specific Vulnerabilities of Software Assets via manifests of upstream dependencies, links to CVE and other vulnerability databases, which can dynamically update Software Asset Vulnerabilities.
- Threats attack Assets by exploiting Vulnerabilities. As Vulnerabilities increase in Assets, the Assets become more susceptible to Threat attacks.
- A Threat has a base Likelihood determined by intrinsic factors such as its inherent difficulty, and extrinsic factors such as the motivations of actors to attack via this Threat.
- Assets have Consequences, which represent undesirable effects of Threat attacks on Assets. Examples of Consequences include Loss of Confidentiality, Integrity of Availability for data.
- A Consequence has a Likelihood, which is determined by the causing Threat Likelihoods combined with the Vulnerabilities of the attacked Asset that are exploited by the Threat, considering the presence or absence of defensive capabilities on the Asset that lower or raise its Vulnerabilities respectively. Many Threats may lead to the same Consequence on the same Asset, in which case the highest (worst case) Threat Likelihood determines the resulting Consequence's Likelihood.
- A Consequence has an Impact level that represents the severity of the type of Consequence on the affected Asset.
- A specific Consequence on an Asset has an associated Risk Level. The Risk Level is determined by the Consequence's Impact Criteria (determined by judgement) combined with its Likelihood (determined by the likelihood of its causing Threats).
- Controls modify Risk levels by introducing defensive measures to Assets that reduce their Vulnerabilities. Via this mechanism, the Consequence Likelihoods reduce.

In summary, SBOMs provide transparent means of determining Software Asset Vulnerabilities. Threats link Vulnerabilities to Consequences on Assets (which determines Risk Level) and Consequences are addressed by Controls.

X. Concluding Remarks

We have presented the Software Bill of Materials (SBOM) concept, and argued for why it will be important in critical infrastructure going forward. We have also highlighted challenges related to risk assessment and SBOM. We have identified *automation* as one of several important aspects for SBOM use, and this is one are we will tackle in further work in the Horizon Europe TELEMETRY project.

Acknowledgements

This work has been supported by the Norwegian Research Council through SFI NORCICS, grant number 310105, and the Horizon Europe project TELEMETRY, grant number 101119747.

References

[1] Fossa, "6 takeaways from the Linux Foundation's SBOM report," https://fossa.com/blog/6-takeaways-linux-foundations-sbom-report/.

[2] C. Nissen, J. E. Gronager, R. S. Metzger, and H. Rishikof, "Deliver uncompromised: A strategy for supply chain security and resilience in response to the changing character of war," MITRE CORP MCLEAN VA, Tech. Rep., 2018.

[3] M. G. Jaatun and H. Sæle, "A checklist for supply chain security for critical infrastructure operators," in *Proceedings of the 2023 Cyber Science Conference*, 2023. [Online]. Available: https://jaatun.no/papers/2023/A_Checklist_for_Supply_Chain_Security.pdf

[4] R. A. Martin, "Visibility & control: addressing supply chain challenges to trustworthy software-enabled things," in *2020 IEEE Systems Security Symposium (SSS)*. IEEE, 2020, pp. 1–4.

[5] J. Hagen and H. Fridheim, "Når sikkerheten er viktigst—beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner," https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/sec4.

[6] S. Coughlan, "What is an SBOM?" https://www.linuxfoundation.org/blog/what-is-an-sbom/.

[7] ISO, "Information technology – IT asset management — part 2: Software identification tag," ISO/IEC Standard 19770-2:2015, 2015. [Online]. Available: https://www.iso.org/standard/65666.html

[8] The White House, "Executive order on improving the nation's cybersecurity," https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[9] NSM, "Grunnprinsipper for ikt-sikkerhet 2.0," https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/.

[10] ENISA, "NIS directive," https://www.enisa.europa.eu/topics/nis-directive.

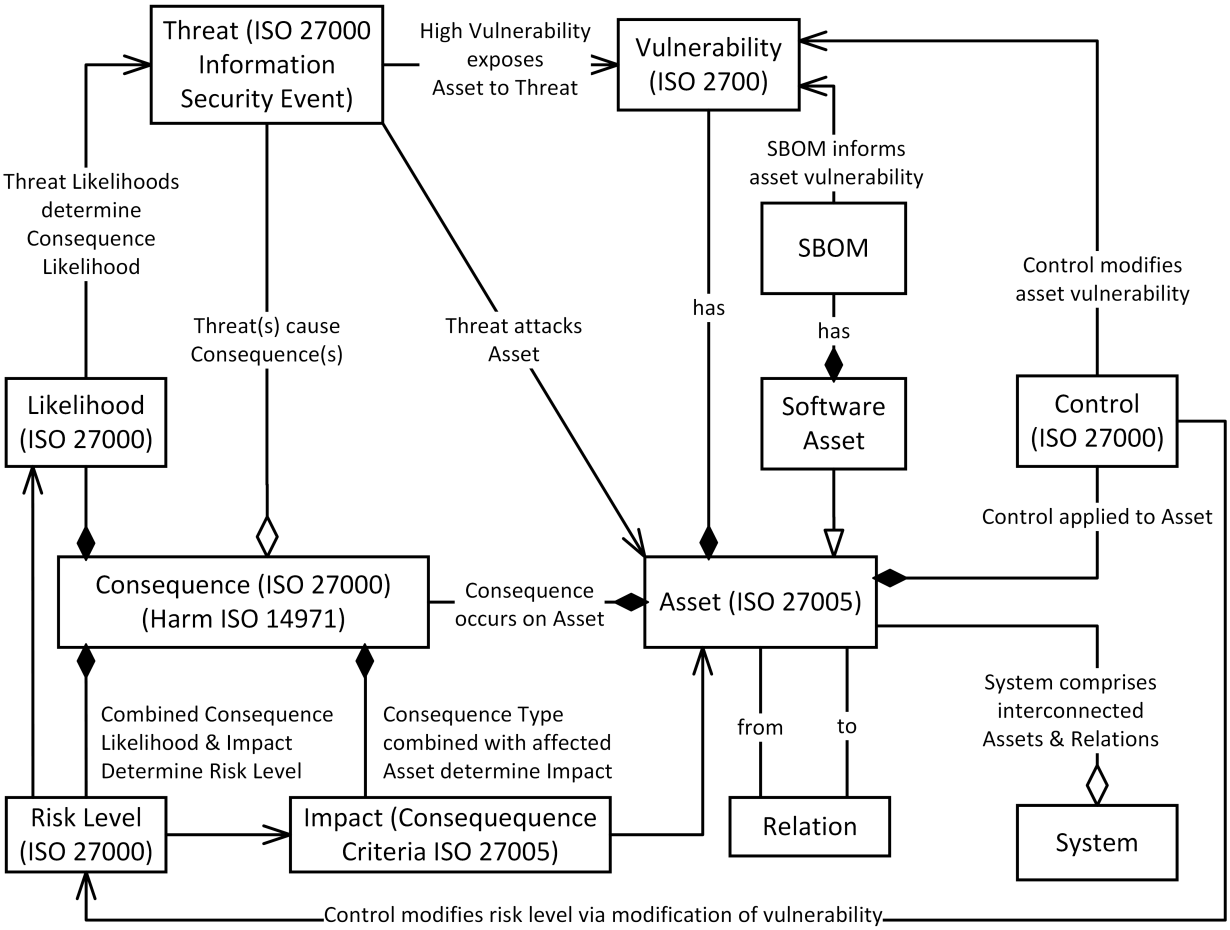

Fig. 1. SBOM in the context of risk

[11] Government of Norway, "NIS-direktivet," https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/.

[12] EU, "Directive (eu) 2016/1148 of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the union," https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[13] Finansdepartementet, "Beredskap i den finansielle infrastrukturen," https://www.regjeringen.no/no/tema/okonomi-og-budsjett/finansmarkedene/beredskap/id2353825/.

[14] Lovdata, "Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)," https://lovdata.no/dokument/SF/forskrift/2003-05-21-630.

[15] S. Livingston, S. Sanborn, A. Slaughter, and P. Zonneveld, "Managing cyber risk in the electric power sector," *Deloitte. As of*, vol. 17, 2019.

[16] Norwegian department of oil and energy, "Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften)," https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157#KAPITTEL_6.

[17] S. Carmody, A. Coravos, G. Fahs, A. Hatch, J. Medina, B. Woods, and J. Corman, "Building resilient medical technology supply chains with a software bill of materials," *NPJ Digital Medicine*, vol. 4, no. 1, pp. 1–6, 2021.

[18] M. Choong, "Principles and practices for medical device cybersecurity," International Medical Device Regulators Forum, 2020. [Online]. Available: https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

[19] LOVDATA, "Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)," https://lovdata.no/dokument/NL/lov/2014-06-20-43/KAPITTEL_2#%C2%A76.

[20] Nasjonal Kommunikasjonsmyndighet, "Tilbyders sikkerhets- og beredskapsplikter," https://www.nkom.no/sikkerhet-og-beredskap/tilbyders-sikkerhets-og-beredskapsplikter.

[21] LOVDATA, "Lov om elektronisk kommunikasjon (ekomloven)," https://lovdata.no/dokument/NL/lov/2003-07-04-83/KAPITTEL_2#%C2%A72-10.

[22] Nasjonal Kommunikasjonsmyndighet, "Kva gjer nkom," https://www.nkom.no/om-nkom/kva-gjer-nkom.

[23] LOVDATA, "Lov om nasjonal sikkerhet (sikkerhetsloven)," https://lovdata.no/dokument/NL/lov/2018-06-01-24.

[24] Nasjonal Kommunikasjonmyndighet, "Net Neutrality in Norway – Annual Report 2021," https://nkom.no/aktuelt/nettnoytralitet-nkoms-arsrapport-for-2021/_/attachment/download/b346d191-1ab4-41b3-9a3c-f28e81694e19:392d5e9cb58efbc1d28fbaa742c447aae0b8fc52/Net%20Neutrality%20in%20Norway%20-%20Annual%20Report%202021.pdf, 2021.

[25] ISO, "Information technology – security techniques – information security management systems – overview and vocabulary," ISO/IEC Standard 27000:2018, 2018. [Online]. Available: https://www.iso.org/standard/73906.html

[26] R. W. Shirey, "Internet Security Glossary, Version 2," RFC 4949, Aug. 2007. [Online]. Available: https://www.rfc-editor.org/info/rfc4949

[27] ISO, "Medical devices – application of risk management to medical devices," ISO Standard 14791:2019, 2019. [Online]. Available: https://www.iso.org/standard/72704.html

[28] ISO, "Information technology – security techniques – information security risk management," ISO/IEC Standard 27005:2018, 2018. [Online]. Available: https://www.iso.org/standard/75281.html