Evaluating Organization Security: User Stories of European Union NIS2 Directive

Mari Seeba[1,2][0000−0002−9066−2467], Magnus Valgre[1][0009−0000−2575−5301], and Raimundas Matulevičius[1][0000−0002−1829−4794]

[1] Institute of Computer Science, University of Tartu, Estonia
[2] Estonian Information System Authority
{mari.seeba, magnus.valgre, raimundas.matulevicius}@ut.ee

Abstract. The NIS2 directive requires EU Member States to ensure a consistently high level of cybersecurity by setting risk-management measures for essential and important entities. Evaluations are necessary to assess whether the required security level is met. This involves understanding the needs and goals of different personas defined by NIS2, who benefit from evaluation results. In this paper, we consider how NIS2 user stories support the evaluation of the level of information security in organizations. Using requirements elicitation principles, we extracted the legal requirements from NIS2 from our narrowed scope, identified six key personas and their goals, formulated user stories based on the gathered information, and validated the usability and relevance of the user stories with security evaluation instruments or methods we found from the literature. The defined user stories help to adjust existing instruments and methods of assessing the security level to comply with NIS2. On the other hand, user stories enable us to see the patterns related to security evaluation when developing new NIS2-compliant security evaluation methods to optimize the administrative burden of entities.

Keywords: NIS2 Directive · Security Evaluation · User Stories · Organizations Security level

1 Introduction

In 2015, the enactment of the European (EU) GDPR data protection regulation changed the attitude toward data privacy and raised awareness of the issue [40]. The impact of the implementation of the GDPR has been global. Similar data protection regulations have now been established all over the world [6]. With the NIS2 Directive, the aim of the EU Commission [8] is to change the information security management postures of organizations in the EU to effectively protect the digital single market, and reduce the damaging impacts of security incidents on the economy and society [8]. Similarly to the enactment of GDPR, a widespread increase in security awareness and implementation of the directive's requirements outside the EU is expected.

From a policymaker's perspective, NIS2 creates explicit measures for entities required to implement the directive's requirements [48,13]. From the perspective

of implementers and engineers, the complexity of interpreting and implementing the regulations is recognized [18,23,11]. For engineers, security is relative, depending on many factors, and the *all-hazards approach* used in NIS2 [8] is an unattainable situation. Therefore, it is appropriate to reformulate the requirements of the regulations into a format understandable to engineers. This allows policymakers and implementers to break out of their silos and get involved in a dialogue, and exchange feedback on the practical effectiveness of the directive [32,1]. Additionally, implementing the regulations should not involve reinventing the wheel but rather building on existing standards and solutions for harmonization [41].

In this paper, we focus on one of the NIS2 directive's objectives - achieving a common high level of security across the EU [8]. We narrowed our research area to the evaluation of the implementation level of risk-management measures, which are presented in NIS2 to organizations. We analyzed the regulation to identify who must meet the specified requirements and for what purpose, based on data from the assessment of organizations' information security levels. Ultimately, we elicit user stories related to the results of organizations' information security level evaluation support that meet NIS2 requirements. Using the requirement engineering method, we discovered 6 personas and 10 user stories that are directly related to an organization's security level evaluation results. Identified user stories are the prerequisite for identifying ways for NIS2 implementation.

2 Background

2.1 NIS2

The NIS2 Directive [8] was published in the Official Journal of the EU and entered into force on January 16, 2023. It aims to establish a high level of cybersecurity across the Union to protect the European single market from security incidents that could disrupt the economy and society [8]. NIS2 provides risk-management measures for entities, addresses communication channels and reporting, defines contact points during security incidents, and guides supervisory activities and penalties. The organizations who are required to comply with NIS2 are public or private entities in the high- criticality sectors, such as energy, transport, drinking and wastewater, public administration, digital infrastructure, and others listed in Annexes I and II of NIS2 [8]. Compared to NIS1 (published 2016) the NIS2 added more than 10 obliged sectors. Therefore, the requirements must be explicit to the implementing entities and achievable with reasonable investment and administrative costs. EU Member States (MS) had to transpose NIS2 into local law by the 17th of October, 2024 [8].

Eliciting requirements from a legal text is complicated because (i) the text is fragmented and uses concepts and terminology that are different from software engineering, (ii) requirements can arise from different levels of law (e.g., EU level or the member state level or regulative standard), (iii) imperfection and vagueness of the law and its wording allows multiple interpretations and (iv) dynamics of the law over time [23,18]. To mitigate risks (ii) and (iv), we only

considered the EU-level NIS2 directive, which all Member States must adopt based on the principle of minimum harmonization stated in Article 5 [8]. That means the Member State must adopt NIS2 as the minimum baseline. We do not address the level of Member State's requirements. We only used the version of NIS2 [8] from 2022. To mitigate risks (i) and (iii), we used methods described in Sec 4.1.

2.2   Security evaluation

Various methods and instruments [22,24,35] can be used to assess an entity's security level, which can be done through direct measurements of risk management measures, self-assessments (e.g., security maturity models), or second or third-party evaluations (e.g., audits, penetration testing). More indirect measurements can also be used to assess the level of security, such as counting the number of organizations that hold some kind of security management certificate (e.g., ISO/IEC27001 Information security management system compliance certificates). This study explores how the security level evaluation results of NIS2-obliged entities can be interpreted and applied to evaluate risk-management measures implementation independently of any specific evaluation method or instrument.

3   Related Work

Only six of the 27 Member States (Belgium, Croatia, Hungary, Italy, Latvia, and Lithuania)[3] succeeded in transposing the NIS2 into local law by October 17, 2024. One of the reasons for the delay in this transposition is the different views of lawyers and implementers on the applicability of the legal text.

Juridical publications (e.g., [48,3]) see the NIS2 Directive primarily as an enabler of raising the security levels of the Member States and emphasize sanctions for non-compliance, and describes NIS2 as a regulation with explicit requirements. In the view of the engineers, the intricate structure and complex legal language of the texts cause questions and ambiguities [14,13]. From the legal point of view, the primary concern is about the excessive administrative burden [48]. However, this originates from the separate implementation of every single clause rather than a comprehensive information security management system, which would align with best practices (e.g., the international standard ISO/IEC 27001 controls [19]) and support the entities' whole management system. If the lawyers recommend balancing requirements in implementing regulations [48], legal text analysis by engineers would instead find optimization patterns and holistic models [14,21,13].

There are few references to the analysis of evaluating the security level concerning NIS2. Wanecki et al. [49] developed a cybersecurity model based on NIS2

---

[3] https://dnsrf.org/nis2-transition/ NIS2 transition tracker status by 2024-11-01

but did not cover the evaluation of the achieved security level. The only option mentioned is conducting audits, which only cover essential entities. Grigaliunas et al. [13] created a GDPR, NIS2, and ISO/IEC 27001-based framework that categorizes controls into preventive, detective, and corrective; allowing entities to align their security maturity levels but without considering other stakeholders' expectations on security level evaluations.

Fatema et al. [11] first extracted the relevant legal clauses and eliminated the irrelevant to determine the relevant scope. Hassani et al. [14], using LLM-s for legal compliance analysis, turned attention to legal text sentences that are not separate units. It is essential to follow the sequence, definitions, and cross-references as a whole. It is not an option to treat individual sentences out of context. Here the personas and their relationship models can be helpful. Therefore, the legal text analysis cannot start with extracting relevant information, the entire text of the regulation must first processed.

Legal text ambiguity patterns (lexical, analytical, vagueness, and generality) are described by Alsaadi et al. [1], who studied the EU Medical Device Regulation (MDR) and the Health Insurance Portability and Accountability Act (HIPAA). After analyzing the text, they set a goal to remove the ambiguity by rephrasing the legal requirements into user stories. They used more relevant terms to make user stories unambiguous for engineers and enable discussions about the personas' activities and their purposes.

Based on the previously described references, we performed our requirements elicitation. The method is described in more detail in the next section.

4   Creating User Stories

4.1   Method

We elicited the personas, their goals and dependencies, and user stories. As our study is based on the NIS2 Directive's [8] legal text, we also followed the suggestions on legal text analysis described by [21,11,18].

Following the example of [11], after reading the entire NIS2 directive text, we only selected the clauses relevant to our study. Then we analyzed the sentences individually, marking actors, actions, and resources as suggested by Islam et al. [18]. Following the steps outlined in [21,18], we created the strategic dependency goal model of the personas in i* modelling language [51].

Next, we defined the user stories (see in Sec. 4.4) related to the organization's security level evaluation following the template format proposed by Cohn [4,5]:

```
As a <type of user>, I can <some goal> so that <some reason>.
```

The simple template-based structure is understandable to stakeholders and software engineers by helping to reach a common understanding of the requirements and define the quality guideline [25]. To validate the user stories, we aligned them with existing methods and instruments to demonstrate that the use cases they covered already exist in practice.

4.2   NIS2 requirements elicitation

Our scope is to find from NIS2 the clauses related to organizations' (in NIS2 vocabulary - essential and important entities) security level evaluation. At first, we got acquainted with the whole NIS2 text, and we highlighted the relevant clauses that can be interpreted in the context of security evaluation of entities. We also used searches for keywords such as *ensure*, *level*, *assess**, *oversee*, and *measures* for crosschecking. Keywords were chosen based on interpretation options: at the Member State level, the term *ensure* can be interpreted as requiring the Member State to evaluate and measure entities' security levels. This evaluation process ensures that entities comply with regulations and maintain an expected level of cybersecurity. To get the *oversee*, an activity related to evaluation is needed. A term *level* describes an association with something, which refers to measurement, assessment, or evaluation. We selected string *measure** to find the relationship between risk-management measures, as well as the relationship between measurement. In the Appendix A are shown the filtered clauses, which relate to entities and their security evaluation.

To identify the personas and find their dependencies and goals, we analyzed all selected clauses of NIS2 using [18] legal text analysis model steps. In the legal text, we marked personas or subjects of action as underlined, normative phrases and modal verbs are marked in **bold**, and actions in *italics* like:

Art20(1) "Member States **shall ensure** that the **management bodies of essential and important entities** *approve the cybersecurity risk-management measures taken* by those entities in order *to comply with Article 21*, **oversee its implementation** and can be held liable for infringements by the entities of that Article." [8]

This allowed us to pick out the preliminary mentioned personas (actors): ENISA, European Parliament, peer reviewers, Member State, small and medium-sized enterprises, management bodies of essential and important entities, important entities, essential entities, service providers & suppliers, and competent authority for supervisory.

We excluded the European Parliament from this list as it is outside the scope of organization-level security evaluation. Also, we excluded the organization's internal structure and processes and focused only on the organization as a general entity with its management body and employees. We engaged peer reviews under the Member State persona, as the process of peer reviews is organized at the Member State level in cooperation with cybersecurity experts from at least two Member States. In our security evaluation scope, the essential and important entities differ only in the supervisory context, where essential entities should be subject to a comprehensive supervisory regime (preventative and after security incidents). In contrast, important entities should be subject to a simplified supervisory regime after a security event or someone's hint of an entity security violation. Security level evaluation is similar in both cases. We also included small and medium-sized enterprises under the persona Entity and Suppliers or Service Providers because all Entities can simultaneously be someone's Service Provider & Supplier and essential and important entities.

Additionally to already mentioned personas, from NIS2 recitals No 56, we found the persona called *Member State point of contact* for small and medium-sized enterprises, who should guide and assist small and medium-sized enterprises regarding cybersecurity-related issues. Impersonally, but the same guidance and assistance issue is mentioned as an expected clause of Member State National cybersecurity policy (Art 7(2)(f) and (i) [8]). To avoid confusion with another single point of contact used for different processes described in NIS2, we named this guidance and assistance provider as a Security Consultant.

So, we limited the personas of NIS2, who are relevant in the context of organization security level evaluation with the list: *Member State*, *Supervisory Authority*, *ENISA*, *Entity*, *Security Consultant* and *Service Provider & Supplier*. In the next section, based on legal text analysis, we describe the personas mutual relations goal model.

4.3   Personas' Dependency Model

The six personas rely on organizations' security data or generalized results to achieve their objectives. The goal of the **Member State** is to receive secure services from Entities, obtain the service's security statuses, assign Consultants to support Entities with cyber-security issues, assign a Supervisory Authority and provide guidance and training on cybersecurity to Entities ([8] Articles: Art1(1); Art7(2); Art19(1.a); Art20(1),(2); Art21(1),(2),(3),(4); Art31(2), Art32(2),(4); Art33(2)). **Supervisory Authority** is assigned by Member State. It should provide feedback on Entities' security status ([8] Articles: Art21(1),(2),(4); Art31(2); Art32(2),(4); Art33(2)). **ENISAs'** goal is to evaluate the security status of Member States and Entities and provide results to the EU Parliament so that it could assess the EU security level ([8] Articles: Art1(1), Art18(1)). **Security Consultants** assist and guide Entities on risk-management measures implementation and could be assigned by Member State ([8] Articles: Art 7(2); Art20(2); Art21(2)). **Entity** provides secure services to Member State and follows Member State regulations (implements risk-management measures, passes training). It also gets secure services and products from Service Provider & Supplier ([8] Articles: Art7(2); Art20(1),(2); Art21(1),(2),(3),(4); Art32(2),(4); Art33(2)). **Service Provider & Supplier provides** provide secure services or products to Entity, ([8] Articles: Art21(2); Art21(3)).

We illustrate the above dependencies in Fig. 1. The model emphasizes the personas' dependencies and supports the user stories. For simplification, ENISA is not included. However, as described above, ENISA obtains the security status of the Member State and Entities and shares the best practices with other Member States. The prioritization and optimization of activities is the task of the Supervisory Authority. It should be noted that a specific organization can take different roles. For instance, an Entity can simultaneously be a Service Provider, Supplier, and Security Consultant. In some cases, the Entity can be a Member State or Supervisory Authority (e.g., Computer Security Incident Response Team, CSIRT).
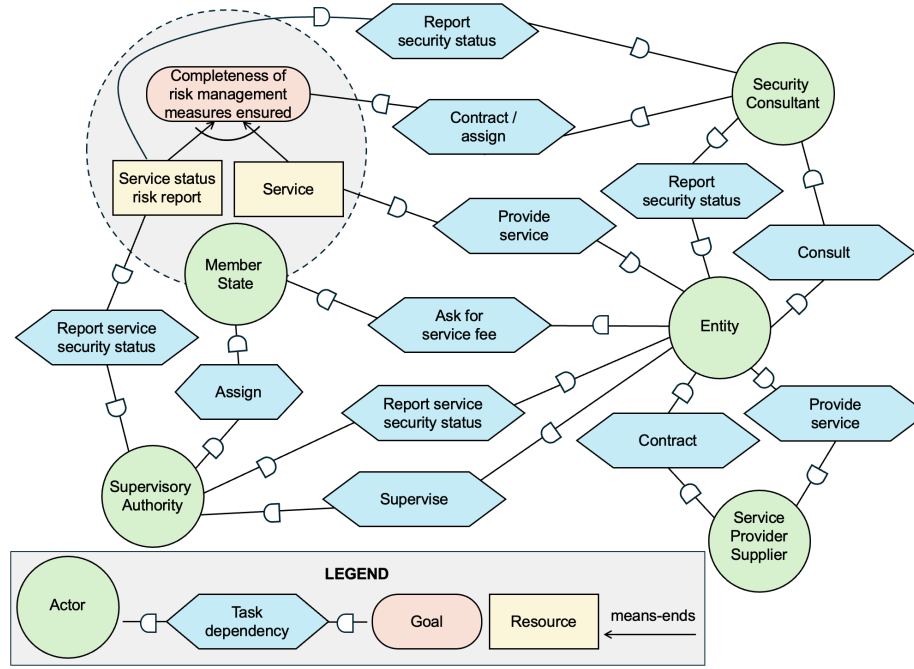
Fig. 1: Personas' Dependency Model

4.4 Security Evaluation User Stories

Next, we describe the User Stories. They are formulated based on the legal requirements quoted in the Appendix A) and the dependencies illustrated in Fig. 1. User Stories are divided into groups based on Personas. The result is presented in Table 1, where the goals regarding security level evaluations are described for each Persona. We also included references to NIS2 clauses.

Table 1: User Stories of NIS2 [8] Related to Security Level Evaluation of Entities

Role:	**Member State**
Goal:	Factual proof of achieving a high common level of cybersecurity in all sectors and entities to avoid cyber incidents causing major damage to economics and society.
Reference:	Art1(1); Art7(2); Art19(1.a); Art20(1),(2); Art21(1),(2),(3),(4) of NIS2 [8]
US1.1: As a Member State, I can oversee the security posture of Entities through structured security level evaluation results, so that I achieve awareness of compliance with regulations.	
US1.2: As a Member State, I can evaluate an entity's cybersecurity level using an all-hazards approach, so that I can allocate resources to address directly on identified vulnerabilities.	

Continuation of Table 1	
Role:	**Supervisory Authority**
Goal:	The Supervisory Authority should base on risk assessments when planning their supervisory tasks, but they should optimize the workflow and not unnecessarily hamper the business activities of the entity concerned.
Reference:	Art21(1),(2),(4); Art31(2); Art32(2); Art32(4); Art33(2)of NIS2 [8]

US2.1 As a Supervisory Authority, I can prioritize supervisory tasks by using all hazard-covering security evaluation results so that I can focus supervisory tasks on high-risk entities or areas.
US2.2 As a Supervisory Authority, I can ensure (with a security evaluation instrument) that entities that did not comply with regulatory requirements implement corrective risk-management measures within reasonable deadlines so that supervisory resources are used effectively and unnecessarily hamper the business activities of the entity is avoided.

Role:	**ENISA**
Goal:	Collect data to evaluate EU security level and report the result to EU Parliament
Reference:	Art1(1), Art18(1) of NIS2 [8]

US3.1 As ENISA, I can collaborate with Member States to assess collected evaluation data on cybersecurity capabilities and awareness, so that I can share cybersecurity best practices and gaps across the European Union.

Role:	**Security Consultant**
Goal:	Consultants should help improve the entity's security level by finding and focusing on vulnerable areas of the entity.
Reference:	Art20(2); Art21(2) of NIS2 [8]

US4.1 As a security consultant, I can get an overview of the entity's security maturity evaluation results so that the most vulnerable areas can be prioritized in a timely manner for an improvement plan.
US4.2 As a security consultant, I can re-evaluate the entity's risk-management measures implementation so that tracking characterizes risk-management measures implementation status progress.

Role:	**Entity**
Goal:	To obtain an overview of the entity's cybersecurity risk-management measures all-hazard approach to confirm security status and improve vulnerable areas
Reference:	Art20(2); Art21(2) of NIS2 [8]

US5.1 As an entity, I can ensure the entity adopts an all-hazards approach[4] to cybersecurity so that the evaluation results show strengths and direct to plan improvements to our security shortcomings.

Role:	**Service Provider & Supplier**
Goal:	Get an evaluation of Service Provider & Supplier security to share with partners and assess compliance with partner requirements
Reference:	Art21(2); Art21(3) of NIS2 [8]

---

[4] Some recognized standard like ISO27001[19] can limit the uncertainty of the all-hazard approach.

Continuation of Table 1
US6.1 As a Service Provider & Supplier, I can provide the risk-management measures in all-hazard evaluation approach results to the partner Entity so that the Entity can choose us as the most suitable secure suppliers.
US6.2 As a Service Provider & Supplier, I can regularly evaluate my cybersecurity practices so that I can present my evaluation results to my partner Entity to demonstrate our security.

To explain the user stories provided in the Table 1, we will take a closer look at how to use user stories and also show how user stories are connected and need additional analysis by the Member State (MS).

US2.1 calls for the Supervisory Authority to prioritize activities in the context of all risks and plan its activities based on this. In essence, this prepares a sample of organizations to focus on. MSs can have several security-related supervisory authorities with different focuses in terms of sectors and functions (e.g., in Estonia, there are three: NCSC-EE, whose supervision deals with cybersecurity in general; the Financial Supervision Authority focuses on the financial sector, and the Data Protection Authority monitors data protection. In Finland, oversight of cybersecurity issues is divided between 8 institutions by area.) Each supervisory unit must prepare its plans based on its objectives and, in addition, national risk assessments.

Therefore, a Supervisory Authority needs aggregated data collected from organizations (reusing the data collected during US5.1) that distinguishes between relevant sectors and their vulnerabilities. This focuses the monitoring process on identifying causes and finding inputs for improvement according to sectors (e.g., finance, energy, research) or security functions (e.g., data protection, incident management, cyber hygiene, and awareness).

However, the MS must specify which metadata must be collected during the US5.1 process for filling in the US2.1 (but also US1.1, US1.2, US3.1). This could depend on MS supervisory authorities, their sectoral affiliation, and how detailed the aggregation needs to be. The questionnaire or instrument detail level should match the supervisory focus needs and data protection requirements, balancing aggregation and listing specific technical measures.

4.5   Validity of User Stories

We validated the user stories by aligning them to existing or proposed security evaluation instruments. The instruments were chosen to cover a wide spectrum of applications and to show that the user stories described in this paper and in NIS2 reflect the situation in the real world. The reviewed instruments can be divided into the following categories: publications [37,2,33,27,34,26,20,50], ENISA or state-sponsored tools [12,9,31,43,42,44,15], cybersecurity indices [10,7,17,47,28], maturity models [46], and official audits [30,29,45].

An overview of the instruments and their coverage of user stories is illustrated in Table 2. Each covers at least one of the user stories. The instruments have been created for different purposes and levels of abstraction. Some instruments

Table 2: Instruments that implement user stories: '+' instrument covers the given user story; '-' instrument does not cover the user story; 'v' instrument can be used to cover the user story, but it is not explicitly meant for that purpose; '*' instrument is not usable *as-is* and needs significant effort to be workable.

Instruments	US1	US2	US3	US4	US5	US6
F4SLE [37], Kybermittari [12], Jazri et al. [20]*	+	+	v	+	+	+
Bernik et al. [2]*, Prislan et al. [33]*, Maleh et al.[27]*, Rae and Patel [34]*, Malaivongs et al. [26]*, You et al. [50]*, self-assessment tools by Ireland [43] and Greece [15], C2M2 Maturity Model [46]	-	-	v	v	+	v
NÚKIB Report[31]*	+	+	-	-	-	-
EU CSI [10]*	+	-	+	-	-	-
Cybersecurity Indices NCSI [7]*, GCI [17]*, NCPI [47]*, CDI [28]*,	+	-	-	-	-	-
Official Audits by Estonia [30]* [29]* and Latvia [45]*	+	v	-	-	-	-
Self-Assessment tools by ENISA [9], IASME [42] and Spain [44]	-	-	-	v	+	v

compare and describe the cybersecurity postures of countries on a global scale (e.g. [10,7,47,28]), while other instruments are meant for individual organizations (e.g. [44,15,43]) and comply with the Entity, Security Consultant or Service Provider & Supplier user stories.

Different abstraction levels require different approaches, which can lead to loss of detail. Cybersecurity indices [10,7,47,28] compare the security postures of entire countries. However, they do not consider the differences in the levels of digitalization, that determines the actual required level of security. Indices rely on high-level data, such as the existence of appropriate legislation and cybersecurity-related institutions, but these facts will not be helpful for individual entities in determining their security level. Still, indices can contain some data on entities (e.g., how many organizations have attained some specific security certifications [10]). The EU Cybersecurity Index [10] created by ENISA uses data gathered from EU member states and is also the subject of US3.

From the bottom-up perspective, most of the methods available are created to help individual organizations perform a self-assessment to find areas of improvement (e.g. [44,42]) and they lack functionality in aggregating data and presenting it at a higher level of abstraction. Still, they fulfill the goals of US5 but can also cover US4 and US6.

The least covered is US2, which means the needs of governmental overseeing bodies are the least considered by the currently available instruments. Two notable instruments here are the audits performed by national audit offices [30,45] and the annual report [31] composed by the National Cyber and Information Security Agency of the Czech Republic (NÚKIB). Due to their thorough nature, audits bring a lot of insight into a given topic and provide concrete recommendations for improvement, but they are not periodically done on the same topic and

this limits their usefulness in verifying that improvements were implemented. The NÚKIB report [31] gathers its data surveys of entities without any individual feedback to the Entity.

There is a real lack of instruments and methods that help collect security evaluation data on individual entities and bring it together for central decision-makers but also, at the same time, provide the given organization with feedback on their current capabilities and areas that need enhancement. In other words, there are only a few tools [12,37] that simultaneously cover the User Stories related to Entities and MSs.

Few security evaluation instruments directly corresponding to NIS2 requirements have yet been created [37,12]. However, an ENISA security assessment pilot report based on NIS2 Article 18 [8] has already been completed, but only for internal use and not publicly available.

The analysis showed that the tools tend to be mono-functional, but some are multifunctional (e.g. [2,43]), simultaneously covering several user stories. Instruments are divided into Member State (US1-US3) and Entity goals (US4-US6). From Table 2, we can see that all our user stories are covered at least by one instrument, showing that user stories are realistic. However, not all instruments are usable for each user story or suitable for periodic/repeatable evaluation.

5   Discussion

A security evaluation aims to provide situational awareness and present the dynamics of security. During the validation of the user stories, we identified different security evaluation methods and instruments which fulfill the needs of either the Member States or the Entities.

Security risk management is an iterative process. If an adversary is able to identify a single vulnerability, they are able to damage the system. However, the Entity (i.e., defender) must implement multiple security countermeasures to mitigate various security risks. This task requires considerable resources. Any activity (including an evaluation of the security level) that does not directly contribute to risk mitigation can significantly burden the organization's administration. Therefore, evaluating the security level should not be a goal in itself; rather, it must be an integrated part of security management and create value for the Entity. We observed four personas (Member State, Supervisory Authority, Consultant and ENISA) who require security evaluation input from entities to support their tasks. The needs of other stakeholders should be integrated into the Entity's security evaluation process. The user stories could help achieve this goal of finding ways to reuse data, optimize, automate, and manage security evaluation, especially from the Entity's point of view.

Finding patterns within legal requirements is the job of experts and engineers. So is optimizing or balancing burdensome activities, as described in Sec. 3 by [14,21,13]. Our research showed that the NIS2 analysis allowed us to find optimization points that could simplify the implementation of NIS2 in a less burdensome way.

Limitation: Our scope is narrowed to NIS2 and does not expand to other EU regulations.User stories follow the NIS2 Directive [8] and are written at a high level of abstraction. This approach allows us to avoid conflicts with the local laws of the Member States when the Member States have transposed NIS2. It also ensures the instantiation of user stories in Member States by adding contextual details. The flexibility of the user stories may lead to challenges in implementation, as they are not explicitly aligned with specific standards or tools.

NIS2 does not refer to any reference standards, the user stories must remain flexible in their application. However, this flexibility may limit the coverage of user stories and their scope in the security assessment. For example, information security management standards (e.g., ISO/IEC27002 [16]) cover the risk-management measures detailed in Article 21(2) of NIS2, but these standards do not specify NIS2-compliant reporting during incidents. Similar concerns are observed for the security awareness training and awareness evaluation of the management boards. However, the Estonian Information Security Standard (E-ITS) [36], a detailed catalog of measures and guidelines, provides corresponding instructions.

The user stories do not explicitly address the continuous compliance required by NIS2, as this is ensured by default through repeated security level evaluations.

6   Concluding Remarks

In this paper, we identified six stakeholders (personas) from the NIS2 directive who depend on the results of an organization's (entity's) security level evaluations to fulfill their tasks. We created user stories that reflect each persona's relation to the evaluation results. The user stories are not dependent on any standards or instruments used for security evaluations. Instead, the user stories are described at the general level.

When adopting NIS2 and planning the security evaluation activities, a Member State should consider how to avoid overloading organizations. Different personas might behave in ways that are based only on their individual needs. The defined user stories could support the planning process by reusing security evaluation results without overburdening the organizations.

Further Work As we are developing the FASLE instrument [37,39,38], we work with stakeholders to test all the described user stories with F4SLE in real-world situations to achieve their operational objectives. This way, we can detail the user stories at the national level to show how they can be implemented with the instrument that collects data only once and uses it for different stakeholders.

Disclosure of Interests. The authors have no competing interests to declare relevant to this article's content.

A   Appendix: NIS2 Extracted and Marked Clauses

Art1(1) "This Directive lays down *measures* that aim to achieve a high common *level* of cybersecurity across the Union, with a view to improving the functioning of the internal market" [8].

Art7(2) As part of the national cybersecurity strategy, Member States **shall** in particular **adopt policies**: (f) promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities; (i) strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible *guidance and assistance for their specific needs*" [8].

Art18(1) requires ENISA **to compile the Report on the state of cybersecurity** in the Union ENISA **shall adopt**, in cooperation with the Commission and the Cooperation Group, a biennial *report on the state of cybersecurity* in the Union and **shall submit and present** that report to the European Parliament. The report **shall**, inter alia, be made available in machine-readable data and **include the following**: (b) an **assessment of the development of** cybersecurity capabilities in the public and private sectors across the Union; (c) **an assessment of the general level of cybersecurity awareness and cyber hygiene** among citizens and entities, including small and medium-sized enterprises; (e) an aggregated **assessment of the level of maturity** of cybersecurity capabilities and resources across the Union, including those at sector level, as well as of the extent to which the Member States' national cybersecurity strategies are aligned" [8].

Art19(1) The peer reviews **shall cover** at least one of the following: a) the **level of implementation of the cybersecurity risk-management measures** /.../ laid down in Articles 21 " [8].

Art20(1)"Member States **shall ensure** that the **management bodies of essential and important entities** *approve the cybersecurity risk-management measures taken* by those entities in order *to comply with Article 21*, **oversee its implementation** and can be held liable for infringements by the entities of that Article." [8].

Art20(2)Member States **shall ensure** that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and *assess cybersecurity risk-management practices* and their impact on the services provided by the entity" [8].

Art21(1) Member States **shall ensure** that **essential and important entities take appropriate and proportionate technical, operational and organizational measures to manage the risks** posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services" [8].

Art21(2) The *measures* referred to in paragraph 1 **shall be based on an all-hazards approach** that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following: a) policies on risk analysis and information system security; b) incident handling; c) business continuity, such as backup management and disaster recovery,

and crisis management; d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers; e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure; f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures; g) basic cyber hygiene practices and cybersecurity training; h) policies and procedures regarding the use of cryptography and, where appropriate, encryption; i) human resources security, access control policies and asset management; j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate" [8].

Art21(3) Member States **shall ensure** that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities *take into account the vulnerabilities* specific to each direct supplier and service provider and the overall quality of products and *cybersecurity practices of their suppliers and service providers*, including their secure development procedures" [8].

Art21(4) Member States **shall** *ensure* that an entity that finds that it does not comply with the measures provided for in paragraph 2 *takes*, without undue delay, *all necessary, appropriate and proportionate corrective measures*" [8].

Art31(2) Member States **may allow their competent authorities to prioritise supervisory tasks**. Such prioritisation s**hall be based on a risk-based approach**. To that end, when exercising their supervisory tasks provided for in Articles 32 and 33, the competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach" [8].

Art32(2) Member States **shall ensure** that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to: a) on-site inspections and *off-site supervision*, including random checks conducted by trained professionals; e) r*equests for information necessary to assess the cybersecurity risk-management measures* adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27" [8].

Art32(4) Member States **shall ensure** that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to: d) order the entities concerned to *ensure* that their cybersecurity risk-management *measure*s comply with Article 21 /.../ , in a specified manner and within a specified period; f) order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline; g) designate a monitoring officer with well-defined tasks **for a determined period of time to oversee the compliance** of the entities concerned with Articles 21 /.../" [8].

Art33(2) Member States **shall ensure** that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to: a) *on-site inspections and off-site ex post supervision* conducted by trained professionals" [8].

Recital (56) Member States **should have** a point of contact for small and medium-sized enterprises at national or regional level, which either *provides guidance and assistance* to small and medium-sized enterprises **or** *directs them to the appropriate bodies* for guidance and assistance with regard to cybersecurity related issues" [8].

References

1. Alsaadi, M., Lisitsa, A., Qasaimeh, M.: Minimizing the ambiguities in medical devices regulations based on software requirement engineering techniques (2019).

`https://doi.org/10.1145/3368691.3368709`

2. Bernik, I., Prislan, K.: Measuring information security performance with 10 by 10 model for holistic state evaluation (2016). `https://doi.org/https://doi.org/10.1371/journal.pone.0163050`

3. Chiara, P.G.: Towards a right to cybersecurity in EU law? The challenges ahead (2024). `https://doi.org/https://doi.org/10.1016/j.clsr.2024.105961`

4. Cohn, M.: User Stories Applied: For Agile Software Development (2004)

5. Cohn, M.: The Two Ways to Add Detail to User Stories (2017), `https://www.mountaingoatsoftware.com/blog/preview/1691`, last access 2024-04-20

6. Dixon, P., Emerson, J.: Global Visualization of Countries with Data Privacy Laws, Treaties, or Conventions, `https://www.worldprivacyforum.org/2024/06/countries-with-data-privacy-laws/`, last access: 2024-11-25

7. e-Governance Academy: National cyber security index. `https://ncsi.ega.ee/`, accessed: 2024-04-12

8. European Parlament: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (2022), `https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555`

9. European Union Agency for Cybersecurity: Cybersecurity Maturity Assessment for Small and Medium Enterprises. `https://www.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises#/`, accessed: 2024-06-13

10. European Union Agency for Cybersecurity: EU Cybersecurity Index. `https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/eu-cybersecurity-index`, accessed: 2024-05-20

11. Fatema, K., Debruyne, C., Lewis, D., OSullivan, D., Morrison, J.P., Mazed, A.A.: A Semi-Automated Methodology for Extracting Access Control Rules from the European Data Protection Directive (2016). `https://doi.org/10.1109/SPW.2016.16`

12. Finnsh Transport and Communication Agency National Cyber Security Centre: Cybermeter. `https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari`, accessed: 2024-05-13

13. Grigaliūnas, S., Schmidt, M., Brūzgienė, R., Smyrli, P., Andreou, S., Lopata, A.: Holistic Information Security Management and Compliance Framework (2024). `https://doi.org/10.3390/electronics13193955`

14. Hassani, S., Sabetzadeh, M., Amyot, D., Liao, J.: Rethinking Legal Compliance Automation: Opportunities with Large Language Models (2024). `https://doi.org/10.1109/RE59067.2024.00051`

15. Hellenic Ministry of Digital Governance Government department: Cybersecurity Self Assessment Tool (2021), `https://mindigital.gr/wp-content/uploads/2022/03/cybersecurity-self-assessment.xlsm`, accessed: 2024-04-27

16. International Organization for Standardization: ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls (2022)

17. International Telecommunications Union: Global Cybersecurity Index. `https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx`, accessed: 2024-05-20

18. Islam, S., Mouratidis, H., Wagner, S.: Towards a framework to elicit and manage security and privacy requirements from laws and regulations (2010). `https://doi.org/10.1007/978-3-642-14192-8_23`

19. ISO/IEC 27001:2022(en) Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Standard, International Organization for Standardization (2022)
20. Jazri, H., Zakaria, O., Chikohora, E.: Measuring cybersecurity wellness index of critical organisations (2018)
21. Jorshari, F.Z., Mouratidis, H., Islam, S.: Extracting security requirements from relevant laws and regulations (2012). `https://doi.org/10.1109/RCIS.2012.6240443`
22. Khaleghi, M., Aref, M.R., Rasti, M.: Comprehensive Comparison of Security Measurement Models (2022). `https://doi.org/10.1080/19361610.2021.1981089`
23. Kiyavitskaya, N., Krausová, A., Zannone, N.: Why eliciting and managing legal requirements is hard (2008). `https://doi.org/10.1109/RELAW.2008.10`
24. Leszczyna, R.: Review of cybersecurity assessment methods: Applicability perspective (2021). `https://doi.org/https://doi.org/10.1016/j.cose.2021.102376`
25. Lucassen, G., Dalpiaz, F., Werf, J.M.E.M.v.d., Brinkkemper, S.: The Use and Effectiveness of User Stories in Practice (2016). `https://doi.org/https://doi.org/10.1007/978-3-319-30282-9_14`
26. Malaivongs, S., Kiattisin, S., Chatjuthamard, P.: Cyber trust index: A framework for rating and improving cybersecurity performance (2022). `https://doi.org/https://doi.org/10.3390/app122111174`
27. Maleh, Y., Ezzati, A., Sahid, A., Belaissaoui, M.: Towards A Capability Assessment Framework for Information Security Governance in Organization (2017)
28. MIT Technology Review Insights: Cyber Defense Index. `https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/`, accessed: 2024-05-12
29. National Audit Office of Estonia: Administration and reliability of X-road. `https://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?FileId=14778&AuditId=2520`, accessed: 2024-11-17
30. National Audit Office of Estonia: Implementation of system of IT security measures in local governments. `https://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?FileId=14270&AuditId=2466`, accessed: 2024-11-17
31. National Cyber and Information Security Agency of the Czech Republic: 2023 Report on the State of Cybersecurity in the Czech Republic. `https://nukib.gov.cz/download/publications_en/2023_Report_on_the_State_of_Cybersecurity_in_the_Czech_Republic.pdf`, accessed: 2023-11-08
32. Pisa, M., Dixon, P., Ndulu, B., Nwankwo, U.: Governing data for development: trends, challenges, and opportunities (2020), `https://www.cgdev.org/sites/default/files/governing-data-development-trends-challenges-and-opportunities.pdf`
33. Prislan, K., Mihelič, A., Bernik, I.: A real-world information security performance assessment using a multidimensional socio-technical approach (2020). `https://doi.org/https://doi.org/10.1371/journal.pone.0238739`
34. Rae, A., Patel, A.: Defining a new composite cybersecurity rating scheme for SMEs in the UK (2019). `https://doi.org/https://doi.org/10.1007/978-3-030-34339-2_20`
35. Rea-Guaman, A.M., Sánchez-García, I.D., Feliu, T.S., Calvo-Manzano, J.A.: Maturity models in cybersecurity: A systematic review (2017). `https://doi.org/10.23919/CISTI.2017.7975865`
36. RIA (Estonian Information System Authority): E-ITS. Portal of Estonian Information Security Standard (2022), `https://eits.ria.ee/`

37. Seeba, M., Mäses, S., Matulevičius, R.: Method for Evaluating Information Security Level in Organisations (2022). `https://doi.org/10.1007/978-3-031-05760-1_39`
38. Seeba, M., amefon Obot Affia, A., Mäses, S., Matulevičius, R.: Create your own MUSE: A method for updating security level evaluation instruments. Computer Standards & Interfaces **87**, 103776 (2024). `https://doi.org/https://doi.org/10.1016/j.csi.2023.103776`
39. Seeba, M., Oja, T., Murumaa, M.P., Stupka, V.: Security Level Evaluation with F4SLE. In: Proceedings of the 18th International Conference on Availability, Reliability and Security. ARES '23, Association for Computing Machinery, New York, NY, USA (2023). `https://doi.org/10.1145/3600160.3605045`, `https://doi.org/10.1145/3600160.3605045`
40. Szczepaniuk, E.K., Szczepaniuk, H., Rokicki, T., Klepacki, B.: Information security assessment in public administration (2020). `https://doi.org/https://doi.org/10.1016/j.cose.2019.101709`
41. Tasheva, I., Kunkel, I.: In a hyperconnected world, is the EU cybersecurity framework connected? (2022). `https://doi.org/10.1177/17816858221136106`
42. The IASME Consortium: IASME Cyber Essentials. `https://getreadyforcyberessentials.iasme.co.uk/`, accessed: 2024-06-13
43. The National Cyber Security Centre of Ireland: Cyber Security Baseline Standards Self-Assessment Form (2023), `https://www.ncsc.gov.ie/pdfs/Cyber_Resilience_Self-Assessment_Framework_Version_1.4_Jan_23.xlsx`, accessed: 2024-05-27
44. The Spanish National Cybersecurity Institute: Herramienta de Autodiagnóstico , `https://adl.incibe.es/#`, accessed: 2024-05-27
45. The State Audit Office of the Republic of Latvia: Can we rely on the access to information systems and the receipt of e-services? `https://www.lrvk.gov.lv/en/getrevisionfile/29525-5Aio6j7MwYsuSG4nKlzFVmCMG0JZircA.pdf` (2022)
46. United States Department of Energy: C2M2 C2M2 V2.1 HTML-Based Tool. `https://c2m2.doe.gov/c2m2-assessment`, accessed: 2024-06-13
47. University of Harvard Belfer Center: National cyber power index 2020. `https://www.belfercenter.org/publication/national-cyber-power-index-2022` (2022)
48. Vandezande, N.: Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor (2024). `https://doi.org/https://doi.org/10.1016/j.clsr.2023.105890`
49. Wanecki, P., Jasek, R., Drofova, I.: The Contribution of the European NIS2 Directive to the Design of the Cyber Security Model (2023). `https://doi.org/10.1109/IDT59031.2023.10194454`
50. You, Y., Cho, I., Lee, K.: An advanced approach to security measurement system (2016). `https://doi.org/https://doi.org/10.1007/s11227-015-1585-7`
51. Yu, E., Giorgini, P., Maiden, N., Mylopoulos, J.: Social modeling for requirements engineering: An introduction (2010). `https://doi.org/10.7551/mitpress/7549.001.0001`