Software Security Patch Management under EU Regulations

A Socio-Technical Study of Organizations' Patching Practices and Challenges under BIO, DORA and NIS2

Master Thesis

Nikhil Daswani

Delft University of Technology

TU Delft

accenture

Software Security Patch Management under EU Regulations

A Socio-Technical Study of Organizations' Patching Practices and Challenges under BIO, DORA and NIS2

by

Nikhil Daswani

Student number: 5049954

In partial fullfillment of the requirements for the degree of

Master of Science
in **Engineering and Policy Analysis**

at Delft University of Technology,
to be defended on Thursday August 28, 2025 at 13:00 PM

Thesis Commitee

First Supervisor:	Dr. Simon Parkin	(OG, TU Delft)
Second Supervisor & Chair:	Prof. dr. ir. Aaron Ding	(ICT, TU Delft)
External Advisor:	David Reusink	(Accenture)

Course:	EPA2942 Master Thesis
Duration:	February, 2025 - August, 2025
Faculty:	Faculty of Technology, Policy and Management (TPM)

TU Delft accenture

Preface

For a long time, I never imagined this day would come. Completing this research marks the end of my academic journey for now, and as I prepare to leave the university, I feel both relief and unease. The path was often unclear, and doubt sometimes made me question if I could finish my project and program. But in the end, the only way forward was to push through. Along the way, I sought motivation, and my curiosity led me in unexpected directions. This is a series of choices I alone am responsible for.

Despite the ups and downs, I still like the vibrancy of university life. There is something uniquely enriching about being surrounded by people driven by passion and knowledge. And when I was physically or mentally tired, I always had two people urging me forward, my parents, whose unwavering support and encouragement kept me grounded, and the rare opportunity to work on research that truly matters. This thesis gave me the rare chance to engage with a topic that is both timely and significant. It allowed me to expand my thinking, and confront challenges that pushed me beyond my comfort zone.

I am deeply grateful to the committee who guided me throughout this research, Simon Parkin, and Aaron Ding. Their diverse perspectives and expertise played an essential role in guiding me and helping me organize my complex thoughts and ideas. I also want to thank my (ex-)supervisors, my buddy, and all my other colleagues at Accenture Security for their their guidance, support, and feedback throughout this process. Their expertise and encouragement has been instrumental in determining the direction and quality of this thesis. All the sparring sessions, conversations and ”coffee chats” will always be appreciated and remembered.

At first glance, this thesis may appear to be just another academic report. But for me, it represents so much more. The goal was never simply to fulfill a requirement or check a box; it was to reflect on my journey, to acknowledge the moments of doubt and growth, and to honor the lessons learned along the way. Being a boy from a small island 7,876 kilometers away, who arrived with only a few aspirations and the hope of completing my degree, I know the degree itself is not my end goal; it’s the experiences and insights gained that I hold most dear.

What I hope this research will demonstrate, more than anything, is the value of an imperfect, winding academic journey. I have come to realize that my decisions, however unconventional they may have seemed at the time, have led to this moment in meaningful ways. Knowledge doesn’t just come to you; you have to go out and seek it. Each of my personal experiences throughout my life have been integral to the person I am today.

This thesis has not only been a space to develop my analytical thinking but also a chance to bring together the diverse threads of my experiences. It marks the beginning of a new chapter in my career, a period of learning, growing, and evolving. I hope this thesis contributes meaningfully to the field, sparking discussions and inspiring new ideas within the academic community. My goal is for it to be both insightful and thought-provoking for its readers.

I owe my deepest gratitude to my family and friends who have supported me throughout this journey. Their love, understanding, and the time we shared have been invaluable. I also feel a sense of regret for those I unintentionally distanced myself from, as I often took the easier route rather than embracing the support they offered.

Now, with this research complete, I look forward to the future with a renewed sense of purpose. The real work is only just beginning. The warm-up phase is over. Time to step into the world.

Nikhil Daswani
Delft, August 2025

“ज्ञानेन तु तदज्ञानं येषां नाशितमात्मनः।
तेषामादित्यवत् ज्ञानं प्रकाशयति तत्परम्॥”

“For those whose ignorance is destroyed by knowledge,
the knowledge reveals the Supreme.”

— Bhagavad Gita 5.16

Executive Summary

Cyber threat actors overwhelmingly exploit known Common Vulnerabilities and Exposures (CVEs) for which patches might already exist, yet the volume of newly disclosed CVEs continues to rise steeply, which threatens critical infrastructure and the wider economy and society. Timely software security patch management (SSPM) remains one of the main measures to prevent threat actors from exploiting such CVEs, but critical large organizations still struggle with applying patches because they face a persistent dilemma: patch too quickly and they risk downtime or compatibility issues; patch too slowly and they invite security breaches such as the Equifax incident. Several human, organizational, and technical factors, also known as socio-technical factors, add to the complexity of patch management by influencing the timeliness and effectiveness of patches, e.g. resource constraints, collaboration, coordination, etc.

Previous software security patch management studies suggest that system administrators patch according to their own planning and design, but regulators have begun to enforce regulatory requirements, by e.g. mandating patching deadlines, to improve cyber resilience. For example, the US CISA KEV catalogue sets a three-week deadline for some organizations in the United States, or the Dutch BIO regulation that sets a one-week deadline for highly critical vulnerabilities for Dutch government organizations. By contrast, the European Union, which is increasingly regulating cybersecurity in an attempt to harmonize cyber resilience across different sectors in the EU, takes a different legislative approach with the introduction of the Network and Information Security 2 Directive (NIS2), and the Digital Operational Resilience Act (DORA). NIS2 and DORA demand “appropriate and timely” patches or mitigation measures for vulnerabilities without prescribing specific patching deadlines. Because no such deadline is given, European legislation still leaves room for interpretation for IT practitioners, which creates uncertainty over what is justified and considered as due diligence.

Therefore, the question central to this research was: ”How do regulations influence organizations’ patch management policies and practices, and how do socio-technical factors interact with these?” To answer this, a qualitative, case study methodology was used. 12 semi-structured interviews were conducted with cybersecurity consultants, and with cybersecurity professionals from two large case study organizations. One organization was an IT/OT manufacturer subject to the NIS2 Directive, and the other organization was a large financial entity subject to DORA. Inductive thematic analysis was used to derive patterns and themes.

Critically, the results reveal that regulations have the potential to be both a constraint and a catalyst. On one hand, the findings firstly show that translating regulations into patch and vulnerability management policies presented significant challenges for when organizations are introduced to new regulations, which are (i) defining the IT landscape that falls under regulatory scope, (ii) resistance from new different teams when regulations bring change, (iii) applying the principle of proportionality, or (iv) poor asset management. However, the study also reveals that previously regulated organizations demonstrated adaptive capacity, and developed workarounds such as stakeholder engagement workshops, iterative timeline setting, mapping of regulations (Appendix E).

The study also shows that socio-technical barriers (such as legacy systems, unclear asset ownership, decentralized organizational structures, limited automation, and cross-team coordination and collaboration), remain deeply persistent. The results consistently showed barriers such as incomplete limited automation, unclear ownership of systems, and the need to coordinate or collaborate across multiple teams. These barriers frequently caused delays in the patching process, specifically for newly regulated organizations. In these organizations, where such barriers persist more often, regulations amplify the barriers, e.g. by increasing the documentation burden without expanding the organization’s capacity to address them. This creates a compliance–resilience gap, in which organizations can comply with regulations by mitigating risks while actually leaving critical vulnerabilities unpatched. The additional

documentation requirements reflect in the reduced patching speed for newly regulated organizations in the initial phases, until they are able to manage socio-technical barriers effectively.

On the other hand, regulations can enable better patching practices. Counterintuitively, findings show that once non-prescriptive regulations are translated to organizational policies, they increased patching speed for these previously regulated large, critical organizations. The regulatory pressure shifts decision-making power upward, with IT and business management functions now playing a decisive role in setting patch priorities, approving exceptions, and aligning patching with business continuity. They also show how in previously regulated organizations, patch management has evolved from a largely technical maintenance task into a strategic governance process, and even indirectly forces organizations to have better documentation and reporting practices and new functions (e.g. as coordinators, maintenance groups, or even staff for being responsive to emerging critical vulnerabilities).

Based on the findings a few recommendations are provided. Newly regulated organizations can assess their own processes based on the proposed workflow in this work and improve it. They can adopt the identified workarounds of previously regulated organizations to ease the translation process and shorten the learning curve. An example is the use of the mapping of regulations onto standards and controls frameworks in Appendix E to alleviate the ambiguity stemming from the principle of proportionality.

Furthermore, a key challenge was resistance from stakeholders withing an organization when regulations bring changes, such as IT teams opposing stricter deadlines out of fear of infeasibility. To work around this, newly regulated critical organizations are recommended to co-design patch policies that are softer and also heterogeneous for different systems. Imposing more realistic timelines based on different systems' characteristics increases feasibility to comply and reduces resistance. The penultimate recommendation advises newly regulated organizations to adopt a risk-based approach that prioritizes critical assets and vulnerabilities, focusing resources on areas that deliver the greatest risk reduction rather than endlessly trying to fix persistent socio-technical barriers such as perfect automation or complete asset inventories. It suggests maintaining capacity to respond quickly to emerging threats and leveraging roles like "security champions" or "change agents" to discourage superficial compliance and promote effective patching.

The last recommendation proposes policymakers and regulators to use soft governance, such as benchmarking and sector-specific cooperation forums, to address regulatory ambiguity and the lack of practical guidance. Benchmarking would allow organizations to compare patch management performance, identify best practices, and help policymakers set realistic patch timelines, while ensuring accessibility for organizations with limited resources. Cooperation forums should foster a shared, non-competitive commitment to security, to enable exchange of knowledge between peer organizations and regulators without creating competitive disadvantages.

In short, this study highlights that effective software security patch management is as much a socio-technical challenge as it is a regulatory one, requiring the joint optimization of policy, people, and technology. All in all, this study expands current knowledge and provides the pathway to ultimately strengthen organizations' defenses and overall cyber resilience.

Contents

List of Figures

List of Tables

1 Introduction

1.1. Background & Context

”Clear and present danger” — that is how global leaders describe cyber threats today, as nearly 40% of World Economic Forum experts warn it threatens the very foundations of the world economy (Lynch, 2021). Cyber threats refer to any malicious attempts to damage, disrupt, or gain unauthorized access to computer systems, networks, or data (Bezzubov et al., 2017; Ujjwal Rao, 2023). These threats can come from various sources, including cybercriminals, nation-states, and hacktivists (Kaur, 2020; Prasad & Rohokale, 2020), and can take many forms such as malware, phishing, ransomware, and denial-of-service attacks (Humayun et al., 2020).

Such cyber-attacks that are successful often exploit known software vulnerabilities (Erdődi & Josang, 2020; M. S. Hoque et al., 2021). In this regard, there has been a rapid increase in new Common Vulnerabilities and Exposures (CVE) discovered over the past few decades, as shown in Figure 1 (Gamblin, n.d.). Because the cyberspace is ”a complex, manmade system at global scale, deeply embedded in the four physical domains of land, water, air and space” (Van Den Berg et al., 2014), successful exploits of CVEs affect developments in all domains, for instance, national security, critical infrastructures and vital services (Y. Li & Liu, 2021). For example, a malware attack on Ukraine’s power grid in 2015 left 225.000 locals without power (Case, 2016) or a failure to patch a critical Apache Struts vulnerability led to the Equifax breach, which exposed sensitive data of approximately 143 million US consumers (Goodin, 2017). Therefore, cybersecurity has become essential to make and maintain progress in global sustainable development (Adebimpe Bolatito Ige et al., 2024; Odumesi & Sanusi, 2023; UNDP & ITU, 2023).

One of the many crucial ways to deal with the rapidly increasing software vulnerabilities shown in Figure 1, is through timely and effective patch management. The concept of security patching or Patch Management, hereafter software security patch management (SSPM), refers to the process of updating software to address security vulnerabilities in systems and applications within an organization’s IT environment (Dissanayake, Jayatilaka, et al., 2022b). It is a widely acknowledged and effective method for reducing software vulnerabilities and risks (Dissanayake, Jayatilaka, et al., 2022b), and it is a domain that has been receiving significant attention in scientific literature. Regular, well-timed application of security patches that are released by software vendors helps organizations keep their assets secure, reliable, and up-to-date with the required features and functionality (Mehri et al., 2023). According to Mehri et al. (2023), it is also essential for ensuring compliance with security policies, regulations and certifications. Examples are the Network and Information Security 2 (NIS2) directive (European Parliament, 2022), the Digital Operational Resilience Act (DORA) (European Union, 2022), or the EU Cybersecurity Certificate (EUCS) (European Union Agency for Cybersecurity, 2020).

Despite recognizing the importance of SSPM, many organizations fail to prevent timely exploitation of vulnerabilities (Ponemon Institute, 2018; ServiceNow & Ponemon Institute, 2020). ServiceNow and Ponemon Institute (2020) report that 48% of organizations experienced data breaches in the past two

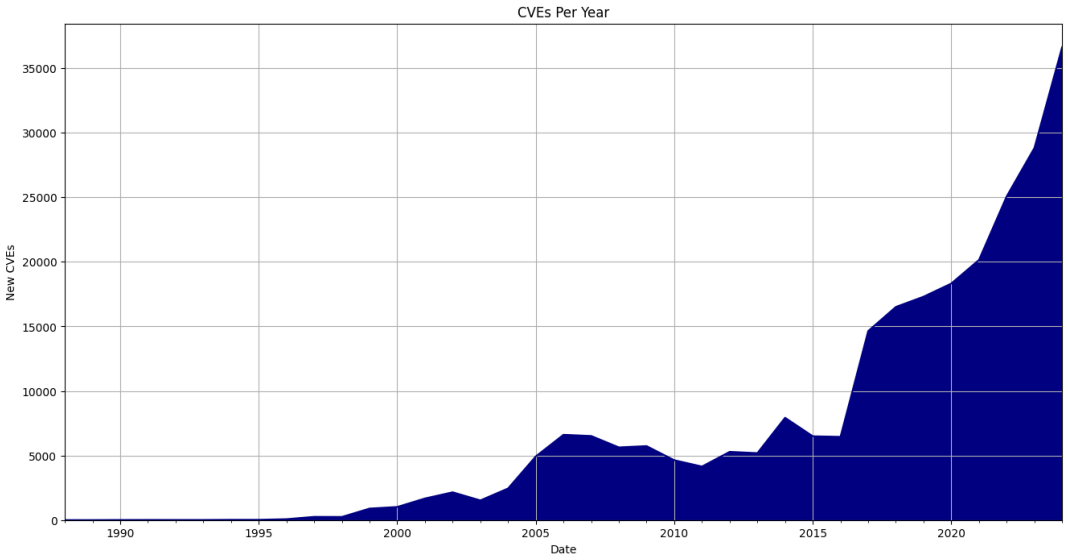

Figure 1: Common Vulnerabilities and Exposures (CVEs) between 1990 and 2024 (Gamblin, n.d.).

years, with 60% attributing these to unpatched known vulnerabilities. Alarmingly, ten Napel et al. (2024) report that only 16.2% of the studied cases completed the patching process within 48 hours, which is considered to be a recommended industry best practice. There is a challenging dilemma organizations grapple with. By patching too quickly, they may risk potential downtime and system failures. Delaying patches leaves them vulnerable to attacks (Beattie et al., 2002; Dissanayake, Jayatilaka, et al., 2022a) that exploit CVEs. This can affect businesses negatively. Consequently, even critical security vulnerabilities often remain unpatched for extended periods.

1.2. Problem Statement

In the past, regulatory guidance has tried to enforce patch management practices. Some examples of regulatory guidance and requirements were mainly provided by the Payment Card Industry Data Security Standard (PCI DSS) (PCI Security Standards Council, 2015), the Society for Worldwide Interbank Financial Telecommunication's (SWIFT) Customer Security Programme CSCF (Society for Worldwide Interbank Financial Telecommunications, 2025), and the European Banking Authority (EBA) Guidelines on ICT and Security Risk Management (European Banking Authority, 2019). However, these instruments offer limited direction with respect to patching cadence or vulnerability prioritization. Moreover, they are advisory in nature and presented as best practices rather than enforceable obligations, and therefore do not exert the same kind of regulatory pressure as seen in more recent legislative frameworks like DORA or BIO. As such, their ability to drive uniform or timely patching practices across the sector has been constrained by their non-binding status.

In response to persistent challenges surrounding vulnerability and patch management, more recent regulations have increasingly aimed to impose clearer expectations and accountability on organizations. For example, the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) Binding Operational Directive 22-01 2021 take a prescriptive approach by enforcing mandatory patching deadlines for vulnerabilities listed in the Known Exploited Vulnerabilities (KEV) catalog. A typical remediation deadline for a new KEV is three weeks and aims to accelerate patching speed and reduce the risk exposure from known threats. A deadline of three weeks might not sound particularly strict, but it represents a substantial acceleration when compared to real-world patching behavior. For instance, Kotzias et al. (2019) analyzed telemetry from 28,000 enterprises and found that it took organizations, on average, nine months to patch 90% of server-side vulnerable systems, with some sectors taking up to two years. While the study does not focus specifically on critical vulnerabilities or the effects of more recent regulatory developments, it emphasizes the considerable gap between expectations set by a mandated deadline and patching practices in large organizations.

A similar approach to the CISA KEV deadline can be found in the Netherlands, where this study takes place, through the Baseline Information Security Government (BIO) framework, which mandates that Dutch government organizations apply patches within one week of receiving a top-priority patch or vulnerability from the national Computer Emergency Response Team (CERT). Like CISA's directive, the BIO framework aims to reduce patching delays by emphasizing urgency and prioritization. Unlike earlier studies such as that by Kotzias et al. (2019), ten Napel et al. (2024) investigated how organizations actually respond to legally mandated patching deadlines. A public sector organization was studied in the Netherlands subject to the BIO framework. The BIO framework enforces a one-week deadline for critical vulnerabilities (Dutch Central Government, 2018; ten Napel et al., 2024). Interestingly, while the organization was unable to consistently meet the required deadlines, the presence of the regulation did lead to significantly faster patching overall compared to typical industry benchmarks (ten Napel et al., 2024).

By contrast, other legislative approaches, such as the European Union's Network and Information Security Directive (NIS2) and Digital Operational Resilience Act (DORA) require critical entities to take 'appropriate and proportionate' technical and organizational measures to manage cybersecurity risks, including the handling of software vulnerabilities. Importantly, DORA and NIS2 also include liability for non-compliance, meaning organizations and their higher management may be held responsible if their actions or inactions are deemed insufficient in the context of identified threats. On the contrary of CISA's directive and the BIO framework, EU legislation does not prescribe fixed patching deadlines which leaves room for interpretation around what timely and proportionate responses really mean.

In the Netherlands, while the BIO framework is legally binding only for public sector entities, they are increasingly promoted as best practices for private enterprises as well. These differences between EU regulations such as the NIS2 and DORA, and other mandates such as the BIO and CISA KEV raise important questions about how organizations interpret, operationalize, and prioritize patching when deadlines are not explicitly imposed but where regulatory scrutiny and liability are still applicable. What effect is such EU legislation having on patch management policies and practices? What challenges in light of EU legislation do organizations face when it comes to patch management? Does regulatory pressure imposed by NIS2 and DORA still actually lead to faster patching speed?

1.3. Research Aim

Although the issue of implementing timely and effective patch management processes has received increasing attention in both regulatory and academic domains, it remains unclear how the absence of strict patching deadlines under regulations such as DORA and NIS2 affects prioritization, timelines, and the regulatory challenges organizations face across different sectors. Previous work, such as the study by Kotzias et al. (2019), has shown that organizations often take many months to patch even known vulnerabilities which shows a significant gap between best practice and actual performance. Dissanayake, Jayatilaka, et al. (2022b) studied the socio-technical challenges organizations face in software patch management. More recently, ten Napel et al. (2024) provided early empirical evidence that mandatory deadlines imposed by regulations can still accelerate patching behavior, even when the strict deadlines are not always met.

Thus, this study aims to bridge the gap between scientific knowledge and industry practices by adopting a socio-technical perspective to examine how organizations interpret and operationalize patch management under the new EU legislation. Given the diverse range of organizations affected by new regulations, this thesis aims to provide actionable insights and recommendations for both policymakers and organizations. It explores key regulatory influences, as well as the technical, organizational, and human factors that shape patch management effectiveness. In doing so, it focuses specifically on critical organizations in the financial sector and IT/OT manufacturing under DORA and NIS2. The recommendations enables organizations in these sectors to more effectively manage software vulnerabilities, align patching practices with evolving regulations, and identify policy or process gaps that can hinder cyber resilience.

1.4. EPA Relevance

By relating this study to the dimensions of EPA Relevance, Table 1 shows how this research on SSPM is linked to the EPA program.

Table 1: Relevance of study to EPA and its dimensions

Dimension	EPA Relevance
Societal Challenge	Software security patch management is one of the many effective ways to prevent cyber-attacks that exploit software vulnerabilities. These exploits affect critical infrastructures, national security, and sustainable development (Adebimpe Bolatito Ige et al., 2024; Y. Li & Liu, 2021). Addressing this challenge through effective SSPM is vital for society at large.
Policy Problem	Software Security Patch Management (SSPM) can be characterized as a *wicked problem* (Head & Alford, 2015; Rittel & Webber, 1973). Wicked problems are complex, difficult to define, and do not have straightforward solutions. SSPM reflects this nature because it spans technical, organizational, and regulatory domains, which require adequate policy interventions. The problem consists of multiple interconnected sub-problems with varying consequences for different actors (Carr & Lesniewska, 2020). Attempts to address one issue often reshape the understanding of others, as every intervention can lead to unforeseen consequences (Mileski et al., 2018; Rittel & Webber, 1973). For example, security patches may introduce bugs (Kansal et al., 2016; Qiang et al., 2017), degrade system performance (Alhubaiti & El-Alfy, 2019), cause compatibility issues (Jabin, 2024; Oberheide et al., 2009), or disrupt operations (Jabin, 2024). This complexity is exacerbated by the rising sophistication and accessibility of cyber threats (Eriksen-Jensen, 2013). SSPM is therefore essential for both mitigating risk and complying with regulations such as NIS2 and DORA (European Parliament, 2022; Mehri et al., 2023). However, effective implementation is hampered by resource constraints, potential downtime, and technical dependencies (Dissanayake, Jayatilaka, et al., 2022b). Because no single actor, or stakeholder within an organization can remediate vulnerabilities or solve challenges of patch management alone, cooperation across sectors, teams, and states is essential (Carr & Lesniewska, 2020; Dissanayake, Jayatilaka, et al., 2022b; Weber & Khademian, 2008). Additionally, although legislation like DORA and NIS2 often avoid prescribing specific patch deadlines, they increasingly expect timely and effective patching, which creates regulatory pressure that must be balanced with operational feasibility. This creates a pressing policy problem for organizations to tackle.
Complex System	Cyberspace is a complex, man-made system embedded in all physical domains, where exploitation of vulnerabilities impacts multiple sectors (Van Den Berg et al., 2014). SSPM involves IT technology, human factors, and organizational dynamics, which requires an analysis of socio-technical interdependencies that cause complexities (Dissanayake, Jayatilaka, et al., 2022b). To add onto this complexity, new regulations are imposing more requirements on organizations, which also needs to be taken into consideration. The interactions between such factors creates complexity that organizations need to manage.
Analytics	The use of semi-structured interviews and thematic analysis in this study relates to EPA's emphasis on analytical tools.
Policy Advise	Synthesis of insights from industry practitioners leads to policy advice and actionable recommendations to guide organizations and IT practitioners in managing software patching challenges more effectively and complying with mandates and regulations. The synthesis of insights also leads to identifying potential gaps or shortcomings in EU legislation on SSPM, which could lead to improved regulations and mandated requirements.

1.5. Report Outline

The remainder of this thesis is structured as follows. Existing scientific knowledge and industry standards on software patching are first synthesized in Chapter 2. Consequently, a knowledge gap and research questions are identified in Chapter 3. Then, Chapter 4 presents a research methodology and design for the collection of semi-structured interview data and the analysis of it with inductive thematic analysis. This design is used to generate new knowledge and insights. Chapters 5 and 6 present the results gained by carrying out the methodology. These results are discussed in light of their implications and their limitations in Chapter 7. Chapter 7 also provides recommendations for large critical organizations and policymakers.

2

State-of-the-art & Literature Synthesis

2.1. Overview of Literature Research

2.1.1. Search Strategy

Scopus was chosen as the sole search engine for identifying relevant primary studies due to its comprehensive indexing of software engineering literature, including sources from databases like ACM Digital Library and IEEE Xplore (Dissanayake, Jayatilaka, et al., 2022b; Kitchenham et al., 2009).

Using Scopus enabled the application of a single, unified search string across titles, abstracts, and keywords to retrieve the most relevant results. Keywords were initially selected from related literature and refined through synonyms and subject headings found in existing studies. These terms were combined using Boolean operators (AND, OR) to create multiple search string variations.

To ensure no potential studies were missed, no time restrictions were applied. The search string was iteratively refined based on the initial research question outlined in Section 1.1 and is presented below. Additionally, backward and forward snowballing was applied to key publications to gather further relevant studies. The search contains literature published until the 3rd of December, 2024.

Search Strings:

- (software OR application) AND (security OR cybersecurity) AND (patch*) AND (management or socio-technical) AND (vulnerabilit* OR CVE*)
- (software) AND (security) AND (patch) AND (management)

Aside from scientific literature, this study also includes a review of relevant industry standards that influence software security patch management (SSPM). Industry standards provide practical guidance and normative expectations for organizations seeking to improve their patching practices. Including these standards in the literature review allows for a more comprehensive comparison of regulations, scientific literature, and organizations' practices.

2.1.2. Study Selection

This strategy yielded several hundred studies. The quality of the reviewed studies was assessed through a systematic screening, using the Covidence application. The screening was based on the studies' relevance to addressing the preliminary question presented in Section 1.1. The studies were assessed based on the inclusion and exclusion criteria presented in Table 2. The number of studies was reduced from 502 to 33, as shown in Figure 2. These 33 studies are shown in Table 4 in Appendix A.

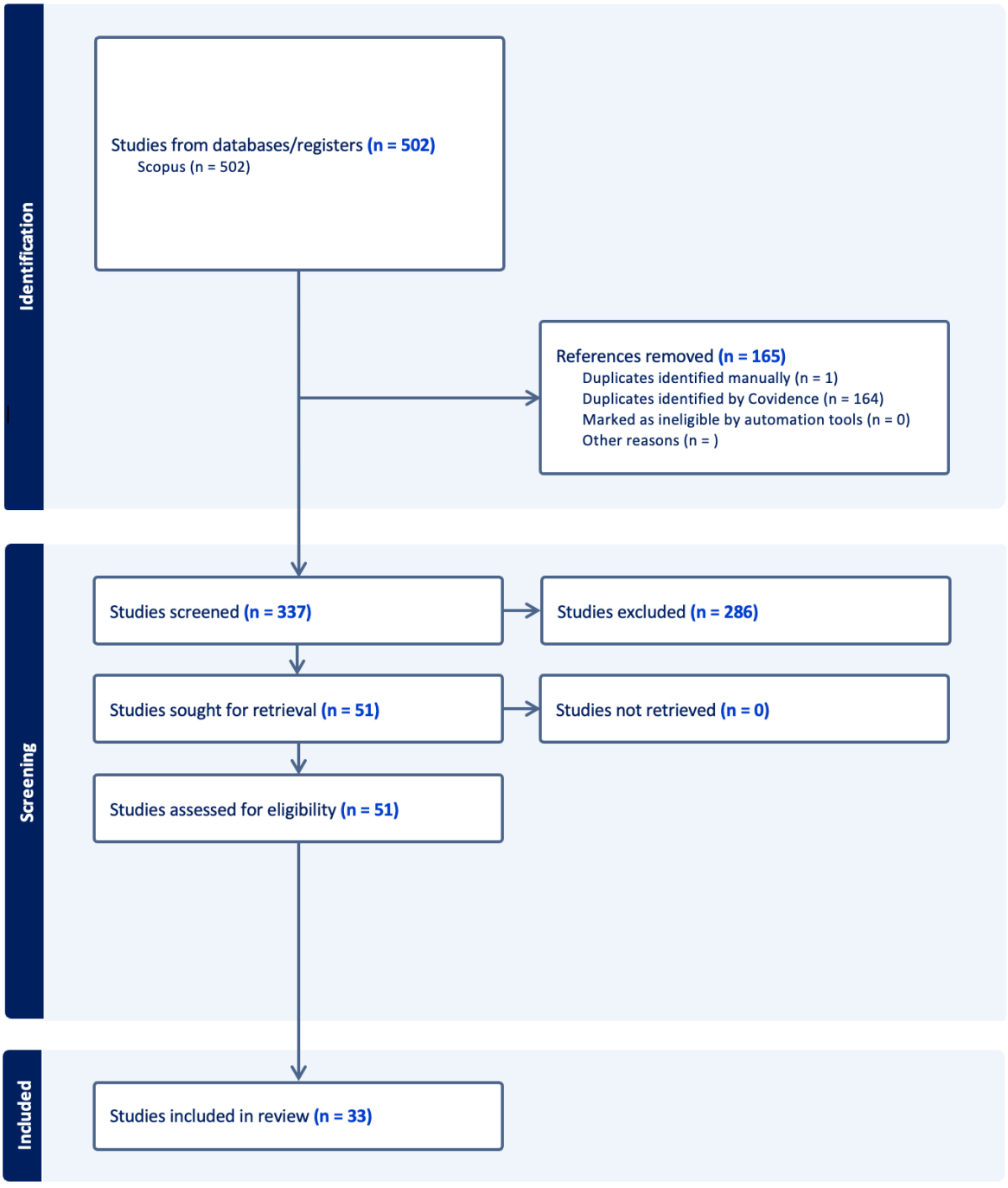

Figure 2: Prisma provided by Covidence showing the identification, screening and inclusion of studies for the literature review

Table 2: Inclusion & Exclusion Criteria for quality assessment of literature

Inclusion Criteria	
1	Full-text peer-reviewed conference or journal articles in English that are accessible .
2	Studies that address at least one phase of SSPM as illustrated in Figure 3.
Exclusion Criteria	
1	Workshop articles, and non-peer-reviewed papers such as editorials, position papers, keynotes, reviews, tutorials, and panel discussions
2	Short papers with fewer than four pages were also excluded.
3	Studies focused solely on numerical analysis, algorithms, or mathematical techniques related to software security patch management
4	Studies only addressing hardware or firmware.
5	Papers outside the domain of software security patch management, as outlined in Figure 3.
6	Studies where the full text was unavailable.

2.2. Review of Scientific Literature

2.2.1. Socio-technical Perspective on Patching

Aside from the studies addressing system administrators' practices and behavior and the problem of timely patch management, the most significant development in academia has been the exploration of various socio-technical factors, challenges, and proposed solutions related to delays in SSPM. According to Bauer and Herder (2009), the socio-technical systems theory highlights the strong interdependence between social and technical subsystems, with socio-technical systems existing at various levels, from individual plants and firms to entire industrial sectors. These subsystems are so closely intertwined that their design necessitates the joint optimisation of both technological and social variables, as Bauer and Herder (2009) emphasize. Dissanayake, Jayatilaka, et al. (2022b) apply this perspective to patch management and define socio-technical: "where human and technological interactions are tightly coupled, such that the success of SSPM significantly depends on the effective collaboration of humans with the technical systems." This highlights the interactions between social and technical components in SSPM. Considering that both social and technical elements are involved in this research, it is essential to explore how technical systems interact with social components during security patching. For this reason, socio-technical system theory serves as the analytical framework for this study.

Using this perspective, Dissanayake, Jayatilaka, et al. (2022b) systematically reviewed literature on SSPM, focusing not only on the overall process of SSPM but also on the various sub-processes involved. Dissanayake, Jayatilaka, et al. (2022b) define SSPM as "a multifaceted process of identifying, acquiring, testing, installing, and verifying security patches for software products and systems." The sub-processes of SSPM are shown in Figure 3 (Dissanayake, Jayatilaka, et al., 2022b; F. Li et al., 2019; Tiefenau et al., 2020). An overview of socio-technical challenges and coping strategies by Dissanayake, Jayatilaka, et al. (2022b) is shown in Appendix B.1. Furthermore, insights of several socio-technical factors that affect the effectiveness of SSPM were also previously identified by van Engelen (2022), as shown in Appendix B.2. All in all, looking at SSPM through a socio-technical lens requires studying the different human, organizational and technical factors and challenges involved.

2.2.2. Technical factors in SSPM

Patching involves significant technical challenges that require careful consideration. Organizations must manage hundreds of patches weekly, requiring multiple steps to ensure successful deployment (Cavusoglu et al., 2006). Each patch carries inherent risks, as untested patches can introduce conflicts with existing systems, leading to technical dependencies between software and hardware (Cavusoglu et al., 2006; Dissanayake et al., 2021). Deployment failures, including faulty configurations or unexpected system changes, may cause downtime and service disruptions (Dissanayake, Jayatilaka, et al., 2022b). Furthermore, some patches fail to address the intended security vulnerabilities, necessitating continuous monitoring and validation.

Since patching every vulnerability is unrealistic, organizations prioritize patches based on risk assessments. High-risk vulnerabilities are addressed first, while lower-risk vulnerabilities may be delayed or ignored, leading to outdated software persisting within IT systems (Andrew, 2005; Dissanayake et al.,

2021). Related to this, Zhu et al. (2011) propose a model for supporting patch deployment decisions.

A further complication arises from the evolving nature of IT environments. The increasing interconnectivity of devices within organizations introduces additional patching complexities. With devices constantly being added, renamed, or removed, tracking and managing patches becomes increasingly difficult (Gerace & Mouton, 2004).

2.2.3. Human factors in SSPM

Human factors play a critical role in SSPM and influence decision-making, coordination, and the efficiency of the patching process. One of the earliest studies examining human factors in system administration was conducted by Hrebec and Stiber (2001), who explored the mental models and situational awareness of system administrators (sysadmins). Many sysadmins lacked formal education in IT and relied on self-developed problem-solving techniques to manage complex systems (Hrebec & Stiber, 2001). The heterogeneous nature of IT infrastructure further complicated their ability to fully understand the systems they managed (Hrebec & Stiber, 2001).

Expanding on this, Barrett (2004) reinforced the issue of situational awareness, noting that sysadmins often struggled to maintain a comprehensive understanding of their IT environments. This lack of awareness increased the likelihood of misconfigurations and security vulnerabilities (Barrett, 2004). Similarly, Dietrich et al. (2018) identified missing or delayed security updates as a major cause of system misconfigurations which further emphasizes the role of human factors in SSPM.

The decision-making process behind patching also involves timing considerations. One of the earliest studies by Beattie et al. (2002) found that sysadmins frequently delay patch installations as it allows them to observe potential stability issues and install a more stable, corrected version if initial releases contain bugs. This ”wait and watch” approach was seen to be potentially advantageous. Jenkins et al. (2024) noted that sysadmins actively seek information from personal networks and forums before deciding to apply patches. However, when they lack particular (patch-related) knowledge, they often rely on third-party support for information on the impact of a patch (Tiefenau et al., 2020). Human factors such as lack of training or insufficient technical knowledge influence patching decisions and contribute to delays or ineffective patch management (Tiefenau et al., 2020).

Another human aspect that complicates SSPM is the way information is gathered and retrieved. F. Li et al. (2019) found that sysadmins lack a centralized platform for retrieving patch-related information which leads them to depend on multiple, and often fragmented, sources. Additionally, when encountering faulty patches, many choose to uninstall the patch and revert to a previous stable state rather than troubleshooting the error and remediating the vulnerability (F. Li et al., 2019). This causes a prolonged exposure to vulnerabilities.

To alleviate this problem, automation tools have been introduced in order to streamline patching. Yet manual patching and ’human-in-the-loop’ remains necessary, specially in dynamic IT environments where human involvement is required (Dissanayake, Jayatilaka, et al., 2022b). However, manual deployment and human involvement introduces human errors which can further delay the deployment of patches and remediation of vulnerabilities (F. Li et al., 2019).

Lastly, collaboration and coordination are also crucial in SSPM. The fundamentally collaborative nature of system administration has been emphasized before (Dissanayake, Jayatilaka, et al., 2022b; Dissanayake et al., 2021; Jenkins et al., 2024). Jenkins et al. (2024) described system administration as an inherently team-based effort, noting that modern IT systems are composed of numerous interdependent components managed by different teams of administrators with specialized expertise. As a result, collaboration across teams is a frequent and necessary aspect of system administration, as administrators must coordinate their actions to maintain and secure complex IT environments. Dissanayake et al. (2021), using a grounded theory approach, also examined how constraints within organizations disrupt coordination efforts, ultimately affecting the efficiency of the patching process. Internal team dynamics affect patching efficiency, as responsibilities among security managers, engineers, and administrators are not always clearly defined (Dissanayake et al., 2021). The lack of clarity in who is

responsible for what and at what stage can lead to inefficiencies and delays. All in all, collaboration, coordination, and communication between different teams are crucial for timely and effective patching (Dissanayake, Jayatilaka, et al., 2022b; Dissanayake, Zahedi, et al., 2022).

2.2.4. Organizational factors in SSPM

Beyond technical and human factors, organizational factors significantly influence patch management decisions. The study by De Smale et al. (2023) found that there was limited respondents had a thorough approach to gathering information on software vulnerabilities, including aggregated sources like the National Vulnerability Database. They also revealed both implicit and explicit coping strategies that organizations use to manage and filter vulnerability information and highlighted three key trade-offs (De Smale et al., 2023). A concerning discovery was the incomplete gathering of knowledge regarding published vulnerabilities. The need for a more structured evaluation process and formal risk management in handling vulnerability information was emphasized (De Smale et al., 2023).

A potential explanation could be that security often competes with other business priorities which requires organizations to balance minimizing service interruptions with maintaining cybersecurity (Dissanayake, Jayatilaka, et al., 2022b). Shostack (2003) explored the decision-making process behind patching. Sysadmins compare the potential risks of installing a patch, such as system failures, compatibility issues, or operational disruptions, against the risks of leaving a system vulnerable to exploits (Shostack, 2003). Research on SSPM has consistently highlighted the challenge of balancing the costs, benefits, and risks associated with patching. Jenkins et al. (2024) emphasized that sysadmins must continuously weigh these factors when deciding whether and when to apply patches. This risk assessment is particularly critical when dealing with core business processes and mission-critical systems, where an faulty update can cause major disruptions.

Another trade-off relates to managing and navigating IT infrastructure when having to ensure security and compliance comes at the expense of user accessibility or operational continuity (Min Khoo & Robey, 2007; Vitale et al., 2017). Vitale et al. (2017) confirmed earlier findings by Min Khoo and Robey (2007) by demonstrating that sysadmins often prioritized security considerations and software licensing issues over the potential consequences for system usability or accessibility.

Dissanayake, Zahedi, et al. (2022) extended their previous research by investigating how and why patches are delayed. This study highlighted the role of organizational policies and schedules, which can sometimes force delays due to operational needs, such as ensuring critical services remain accessible and minimizing downtime. In line with these findings, Kraemer and Carayon (2007) identified that organizational structures and policies play a significant role in determining how security patching is handled. Factors such as company culture, leadership priorities, and predefined maintenance schedules influence the way sysadmins and IT teams approach security updates. Organizational policies and management attitudes toward security can shape patching behavior considering that a strong security culture encourages sysadmins to implement patches more effectively (F. Li et al., 2019).

The availability of security resources also plays a crucial role; greater support from top-level management can lead to higher investment in preventive measures and improved cybersecurity. Moreover, patch management is a collaborative effort involving multiple stakeholders, including vendors, end-users, and IT teams (Dissanayake, Jayatilaka, et al., 2022b). Conflicting interests and interdependencies, such as delays in patch releases from vendors, can create tensions in the process. Effective communication is essential in this case. Additionally, the growing number of connected devices within organizational networks further complicates patching, as devices are constantly added, renamed, or removed (Gerace & Mouton, 2004).

2.2.5. Regulatory factors in SSPM

In recent years, the emergence of cybersecurity regulations has introduced new mandates and expectations that force organizations to reassess the speed and consistency with which they remediate vulnerabilities. While prior studies, such as Kotzias et al. (2019), have shown, for example, that patching 90% of vulnerable systems in enterprise environments can take up to nine months, these analyses were conducted before the implementation of mandated patching deadlines. As a result, their work

provides limited insight into how regulatory requirements influence patch management timelines.

To address this gap, the study by ten Napel et al. (2024) presented one of the first empirical investigations into the effects of binding patching deadlines imposed by national policy. The paper focuses on Dutch public sector organizations governed by the BIO (Baseline Information Security Government) framework, which mandates patching within one week for critical vulnerabilities after a top-priority alert from the national CERT.

By analyzing thousands of ticketing records and conducting follow-up interviews with SOC analysts and technical managers, ten Napel et al. (2024) reveal that while such regulatory patching deadlines are often missed, they nonetheless act as accelerators in mobilizing resources and attention from higher management. When a patch is linked to a so-called “CERT event” (a top-priority advisory), organizations often initiate escalated responses that fast-track deployment and improve monitoring, even if the one-week deadline imposed by the BIO regulation is not always met (ten Napel et al., 2024). This suggests that regulatory pressure can alter patching behavior and speed, not necessarily through perfect compliance, but by introducing a sense of urgency and structure that may otherwise be lacking (ten Napel et al., 2024).

Furthermore, ten Napel et al. (2024) emphasize the risk of aspirational policies becoming liabilities. For example, if an organization consistently fails to meet its own mandated patching deadlines (or those imposed by regulation), these gaps can backfire during post-incident investigations, which exposes them to potential sanctions or reputational damage. In this context, the authors argue for “best practices that are actual practices”. In this case, they refer to the danger of over-ambitious policies that lack actual feasibility.

2.3. Review of Standards, Policies & Regulations

Various advisory and standardization bodies provide support for organizations in security patch management by publishing guidelines and recommendations. These publications, will be used in the analysis of this study based on the availability of information. However, it is important to note that the publications used are not exhaustive, and additional organizations may have released similar publications on patch management practices.

2.3.1. Standards

* ISO27002 series

The ISO/IEC 27002 series of standards (ISO/IEC, 2013, 2022) provide guidance on patch management as part of information security management systems. The ISO/IEC 27002 standard serves as a reference and guidance framework, enabling organizations to develop their own policies and implement effective information security controls. This widely adopted standard has been referenced by the European Union Agency for Network and Information Security (ENISA) to establish requirements for testing and certifying SCADA system updates (European Network and Information Security Agency ., 2013). The report by European Network and Information Security Agency . (2013) outlines key principles derived from the standard, which include:

- Ensuring that the update process does not interfere with the normal operation of the patched devices.
- Minimizing downtime if service interruptions are expected during patch deployment.
- Implementing redundancy in the infrastructure by first applying updates to passive redundant assets. These assets should then be tested in an active state before rolling out the update to the production environment.
- Establishing a dedicated working group responsible for overseeing the patch management process, including:
  - Evaluating potential cybersecurity risks introduced by the patch.

  - Planning and scheduling the patch deployment.
  - Conducting testing, installation, and validation of patches on target systems.

While the level of detail provided in ISO/IEC 27002 is not very extensive, it has been effectively implemented across other industries, e.g. healthcare (Tyali & Pottas, 2010).

* NIST Special Publication (SP) 800-40 series

The NIST 800-40 series by Souppaya and Scarfone (2022) builds upon the content of its earlier publications, serving as sequels that expand on previous work such as Mell and Tracy (2002), Mell et al. (2005), and Souppaya and Scarfone (2013). While the initial publication by Mell and Tracy (2002) covers the fundamental aspects of security patching, the most recent update by Souppaya and Scarfone (2022) assumes that readers are already familiar with these basics. The fourth revision of NIST Special Publication (SP) 800-40 represents the latest approach to enterprise patch management planning. Developed by Souppaya and Scarfone (2022), this publication aims to enhance organizational patch management strategies by strengthening asset management, vulnerability handling, and risk response planning. The key message of the document is that patch management should be viewed as a proactive maintenance process essential for maintaining an organization's technological security.

NIST SP 800-40r4 operates on the premise that organizations can benefit more from refining their patch management planning rather than solely focusing on technological advancements in patching. This assumption is based on the availability of various enterprise-level resources for software vulnerability management. Given the extensive guidance and best practices that have been published over the years by credible institutions like NIST, organizations are expected to have the theoretical capability to implement robust patching strategies. The standard seeks to bridge the gap between business objectives and security needs, which often pose challenges to effective patching.

The publication highlights the evolving cybersecurity threat landscape by emphasizing that vulnerabilities are increasing, cybercriminals are becoming more sophisticated, and the cost of mitigating risks is rapidly escalating. Previously rare threats are now occurring more frequently due to advancements in attack methods, greater exposure, and stronger incentives for attackers. This growing trend underscores the need for organizations to improve their ability to protect assets and implement creative solutions to mitigate risks.

Despite the rising importance of patching, organizational leadership often hesitates to invest in it, thereby compromising software integrity and overall operational efficiency. NIST SP 800-40r4 seeks to address this challenge by offering organizations practical guidance for developing streamlined and effective patch management strategies. Among the various publications on patch management, Souppaya and Scarfone (2022) stand out for providing actionable guidance.

The publication outlines three key benefits of following its guidance (Souppaya & Scarfone, 2022):

- Enhancing the understanding of security and technology management personnel regarding the role of patching in enterprise risk management. Rather than presenting a one-size-fits-all solution, it acknowledges the complexity of decision-making in patch management, highlighting the inevitability of trade-offs. By addressing patching as a risk management challenge that requires engagement at all organizational levels, this publication offers a more relevant and practical perspective on the modern challenges organizations face in patching, making its guidance particularly valuable.
- Improving communication between security teams and business leadership to facilitate better patch management planning. Unlike other works that treat organizational patching as a rigid, well-defined process, this publication takes a broader approach by emphasizing the involvement of multiple stakeholders and the conflicting interests that influence patch deployment planning.
- Equipping organizations with the tools needed to reassess and strengthen their enterprise patching strategies throughout the entire patch management lifecycle.

* IEC TR 62443

The IEC TR 62443 (IEC, 2015) is one of the most widely adopted reference standards for Industrial Control Systems (ICS) across various application domains (Gentile & Serio, 2019). While it offers recommendations on multiple aspects of ICS security, Part 2-3 specifically addresses patch management processes, and could therefore be useful and applicable in a broader sense. IEC 62443 outlines essential guidelines for establishing an effective patch management process, helping to mitigate the risk of unforeseen negative consequences.

2.3.2. EU Policies & Dutch Guidelines

* Network and Information Security 2 (NIS2)
  & the Dutch Cyber Security Act (Dutch: Cyberbeveiligingswet (CBW))

The original NIS directive marked a crucial step in strengthening cybersecurity across the EU, but its implementation varied among member states. In response to the growing volume and sophistication of cyber threats, the European Union (EU) introduced NIS2 (European Parliament, 2022) to enhance security measures, improve supply chain protection, streamline reporting requirements, and enforce stricter supervision and compliance. NIS2 also refines entity classification into essential or important categories and expands its scope to include additional sectors such as wastewater management, food, and space, covering all medium to large companies within these industries.

The NIS2 directive does not specify exact patching deadlines but enforces risk management practices that include vulnerability identification, disclosure, and mitigation. The NIS2 directive emphasizes the critical role of vulnerability assessment and patch management. For example, Article 6 specifically addresses the need for a vulnerability registry that details affected products or services, relevant circumstances, and available patches. It also outlines the necessary measures organizations must take when patches are unavailable.

All EU member states must comply with the NIS2 Directive, which expands upon the original Network and Information Security (NIS) Directive to enhance cybersecurity resilience across key sectors. In the Netherlands, organizations classified as Providers of Essential Services must take immediate action to meet the obligations outlined in the Cyber Security Act (Dutch: Cyberbeveiligingswet (CBW)) (National Cyber Security Centre, 2023a). The NIS2 directive, and its transposition to the Dutch national law CBW, poses some obligations on organizations that fall under this directive:

- Duty of Care (Dutch: Zorgplicht):
  Organizations are required to conduct risk assessments and implement proportionate security measures to protect their network and information systems (National Cyber Security Centre, 2023b). Senior management must approve and oversee these security measures to ensure compliance through proper training and education.
- Incident Reporting Obligation (Dutch: Meldplicht):
  Significant cybersecurity incidents must be reported within 24 hours to the Computer Security Incident Response Team (CSIRT) and the supervisory authority. The directive defines significant incidents as those that could disrupt essential services, cause financial loss, or impact other entities. A centralized reporting system is being developed by the National Cyber Security Centre to facilitate both mandatory and voluntary reporting of incidents (National Cyber Security Centre, 2023a).
- Registration Obligation (Dutch: Registratieplicht) Organizations covered by the Cyber Security Act must register in the national entity register, a system that also contributes to a pan-European database of NIS2 entities. The National Cyber Security Centre is developing an online registration portal to streamline compliance (National Cyber Security Centre, 2023a).
- Supervision and Enforcement (Toezicht) Organizations falling under NIS2 are subject to regulatory supervision, ensuring adherence to cybersecurity requirements such as the duty of care and incident reporting obligations. In extreme cases, executive board members may also be held

accountable for non-compliance (National Cyber Security Centre, 2023a).

* Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act (DORA) establishes a comprehensive framework for managing ICT risks in the financial sector. To ensure its effective implementation, Regulatory Technical Standards (RTS) have been introduced as detailed specifications that expand upon DORA's core requirements. These RTS, developed by the European Supervisory Authorities (ESAs), provide binding guidance on how financial institutions must enhance their digital resilience and comply with DORA's obligations by setting clear technical requirements. Under DORA, the European Commission has the authority to adopt delegated and implementing acts, including RTS, to ensure compliance with the regulation. The European Supervisory Authorities (ESAs), which include the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), and the European Insurance and Occupational Pensions Authority (EIOPA), are responsible for developing and issuing these technical standards. Once adopted, the RTS become legally binding on financial institutions.

The primary aim of DORA's RTS is to harmonize and standardize the way financial institutions across the European Union (EU) manage ICT-related risks, ensuring a consistent approach to cybersecurity and operational resilience. These technical standards cover key areas such as:

- ICT Risk Management – Establishing frameworks for identifying, assessing, and mitigating ICT risks.
- Incident Reporting – Defining mandatory reporting structures, timelines, and content for major ICT-related incidents.
- Digital Operational Resilience Testing – Ensuring institutions conduct periodic testing to assess their preparedness against cyber threats.
- Third-Party Risk Management – Setting requirements for overseeing risks related to outsourcing ICT services.
- Information and Intelligence Sharing – Promoting structured collaboration and information exchange among financial entities to strengthen sector-wide security.

From the aforementioned, but not exhaustive, list, the RTS on ICT Risk Management Framework is a critical component of DORA to ensure financial institutions can effectively mitigate cyber threats. A key aspect of this framework is vulnerability management, which includes identifying, assessing, and addressing security weaknesses in ICT systems. Patch management plays a crucial role in this process, as timely deployment of security patches is essential to prevent exploitation of known vulnerabilities. The RTS sets specific requirements for financial entities, mandating structured patch management processes that include regular updates, risk-based prioritization, and validation procedures to minimize disruptions while maintaining operational resilience.

Therefore, DORA is not just a set of recommendations but a legally enforceable regulation with strict compliance requirements and deadlines for patch management. Meeting patch management obligations and requirements set by the RTS on ICT Risk Management is crucial for financial institutions that aim to strengthen their operational resilience and ensure uninterrupted financial services in the face of cyber threats and ICT disruptions. Non-compliance can lead to regulatory penalties and increased risks for stability of financial systems and services.

* Baseline Information Management Government - BIO (Baseline Informatiehuishouding Overheid)

The Baseline Information Management Central Government (Dutch: Baseline Informatiehuishouding Overheid (BIR)) serves as a key framework for managing government information efficiently and securely. It establishes standards for the Dutch central government to ensure that information is accessible, reliable, and well-organized (Dutch Central Government, 2018). The BIR is designed to support government agencies in improving their information management practices, aligning them with legal

requirements and best practices of information management. The BIR helps central government organizations by providing guidance on measuring and improving information quality, which essentially entails establishing clear benchmarks for assessing the effectiveness and reliability of information systems. It also provides guidance on information management to ensure that data is properly stored, maintained, and made accessible when needed. Moreover, it guides organizations by supporting digital transformations and facilitating the digitization of processes while maintaining compliance with security standards. Lastly, it provides an audit framework, which serves as a reference point for departmental audit services to evaluate information governance.

Since January 1, 2019, the Baseline Informatiebeveiliging Overheid (BIO) has been the standard framework for information security across the entire Dutch government (Centre for Information Security and Privacy Protection, n.d.). It replaces several previous security baselines, including the BIR, as well as frameworks for municipalities, water authorities, and provinces (Centre for Information Security and Privacy Protection, n.d.). Previously, the BIR set security guidelines exclusively for the central government, but the introduction of the BIO extends these principles across all public sector institutions. By consolidating these separate guidelines into a single framework, the BIO establishes a uniform and structured approach to information security and management for all government entities. This transition enhances security, ensures consistency, reduces costs, and fosters better collaboration between government organizations.

The BIO is built upon internationally recognized standards for information security, specifically NEN-EN-ISO/IEC 27001:2017 and NEN-EN-ISO/IEC 27002:2017 (Centre for Information Security and Privacy Protection, n.d.). These standards provide a globally accepted foundation for managing information security risks and implementing effective security controls (Centre for Information Security and Privacy Protection, n.d.). By aligning with these guidelines, the BIO ensures that Dutch government institutions follow best practices in cybersecurity, data protection, and risk management. This includes patch management.

2.3.3. Recommendations Based on Standards & Regulatory Requirements

Analyzing publications chronologically, earlier works primarily focus on conceptualizing security patching, whereas more recent studies emphasize practical implementation strategies for patch management policies. Despite variations in patching processes depending on system type and environmental context, most publications follow a structured, process-oriented approach. A common security patch management process typically consists of five key phases (Dissanayake, Jayatilaka, et al., 2022b) and illustrated in Figure 3. Additionally, there are challenges associated to the overall process of SSPM (Dissanayake, Jayatilaka, et al., 2022b). Accordingly, the remainder of this section is structured to align with the specific phases and with the overall process of patch management.

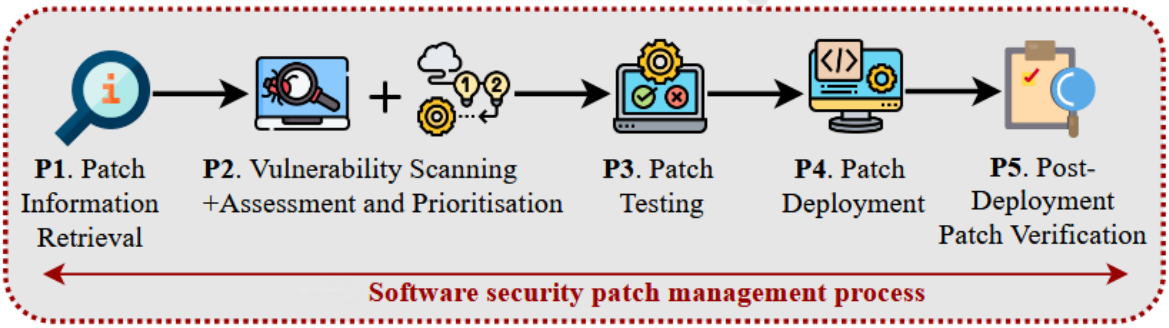

Figure 3: Phases involved in Software Security Patch Management by Dissanayake, Jayatilaka, et al. (2022b)

* Overall Process

Standards on Overall Process

Organizations should recognize that effective patch and vulnerability management is not solely a tech-

nical undertaking but rather a socio-technical endeavor, requiring the integration of well-defined processes, skilled personnel, and appropriate technologies. A foundational element of this integrated approach is the establishment of clear patch policy and process development. Organizations should have explicit and documented patching and vulnerability policies as well as systematic, accountable, and documented sets of processes and procedures for handling patches (Mell & Tracy, 2002). This includes defining what constitutes a vulnerability, the criticality of different types of vulnerabilities, and the expected timelines for addressing them (Mell & Tracy, 2002). Furthermore, these policies should clearly specify the roles and responsibilities of individuals and teams involved in the patch management lifecycle, ensuring accountability for monitoring, testing, and deploying patches (ISO/IEC, 2013; Mell & Tracy, 2002; Souppaya & Scarfone, 2022). It's crucial that personnel are adequately prepared to address problems, understand the reasons behind patching, and comprehend that patching is a necessity for maintaining a secure environment (Souppaya & Scarfone, 2022).

To effectively manage vulnerabilities, organizations must maintain a comprehensive inventory of their IT assets, including hardware, operating systems, software, and configurations (IEC, 2015; ISO/IEC, 2013; Mell et al., 2005). This asset inventory should be kept current and accurate, providing essential information such as vendor details, version numbers, and current state of deployment. Leveraging automation for asset inventory can significantly improve accuracy and efficiency (Souppaya & Scarfone, 2022). This detailed understanding of the IT environment is crucial for conducting thorough vulnerability risk assessment. Organizations should adopt a risk-based approach, prioritizing the remediation of vulnerabilities based on their potential impact and the likelihood of exploitation. This assessment should consider factors such as the affected assets, the nature of the vulnerability, and the availability of mitigations (Souppaya & Scarfone, 2022).

The process of applying patches requires careful planning and execution. Organizations should establish configuration control to ensure consistency across their systems and to minimize the risk of introducing instability through patching (IEC, 2015; ISO/IEC, 2013). Before widespread deployment, patches should undergo thorough testing in non-production environments to ensure compatibility and prevent unintended consequences. This testing phase is critical for validating that the patch effectively addresses the vulnerability without causing disruptions to business operations. Organizations should aim for timely patching, especially for critical vulnerabilities, but must balance speed with the need for adequate testing and validation. In situations where immediate patching is not feasible, temporary mitigations should be implemented to reduce the risk exposure (ISO/IEC, 2022; Souppaya & Scarfone, 2022).

The involvement of third-party software introduces additional complexities to patch management. Organizations should extend their patch management processes to include third-party applications, ensuring that these components are also regularly updated to address known vulnerabilities. Clear communication channels and defined responsibilities are necessary when dealing with vulnerabilities in third-party software (Souppaya & Scarfone, 2022).

Effective patch and vulnerability management also requires consideration of the broader organizational context. Organizations should align their security needs with their business objectives (Souppaya & Scarfone, 2013). Management plays a crucial role in supporting and prioritizing patch management efforts, recognizing it as a fundamental part of enterprise change management. Robust change management policies and processes are essential for ensuring that patching activities are coordinated, communicated effectively, and do not negatively impact business operations. Furthermore, organizations should foster a security-aware culture where personnel understand the importance of patching and are actively involved in maintaining a secure environment (Souppaya & Scarfone, 2022). When dealing with security vulnerabilities, organizations should have well-defined scenario planning processes in place to anticipate potential issues and develop appropriate response strategies (Souppaya & Scarfone, 2022). This includes planning for situations where patches are unavailable, ineffective, or cause unintended disruptions (Souppaya & Scarfone, 2022). Clear procedures for incident response and communication are crucial for minimizing the impact of security incidents related to unpatched vulnerabilities (ISO/IEC, 2022). Organizations should also consider the implications of different deployment scenarios, such as rolling out patches in a phased manner or implementing temporary workarounds (Souppaya & Scar-

fone, 2022). Finally, patch and vulnerability management is not a static process but requires continuous improvement. Organizations should regularly review and refine their policies, processes, and technologies based on lessons learned, emerging threats, and changes in their IT environment (Souppaya & Scarfone, 2022). Staying informed about new vulnerabilities and available patches is an ongoing responsibility. Leveraging automation for various aspects of patch management, such as vulnerability scanning, patch deployment, and inventory management, can significantly enhance efficiency and reduce the risk of human error (Souppaya & Scarfone, 2022).

EU Policies and (Dutch) Guidelines on Overall Process
NIS2 sets the overarching tone by mandating that essential and important entities implement appropriate technical, organizational, and operational measures to manage risks posed to network and information systems. Although the NIS2 Directive is not very specific in this case, it implicitly includes a patch management strategy considering this directly addresses vulnerability mitigation. Furthermore, NIS2 emphasizes basic cyber hygiene practices to improve cybersecurity resilience. Cyber hygiene practices can be interpreted broadly and may contain different elements. Managing the installation of software on operational systems, installing software and hardware updates, and configuration management fall under this. Therefore, it can be reasoned that cyber hygiene practices include patch management as a foundational element.

Given that the NIS2 directive is not very comprehensive and in-depth regarding patch management, its transposition into the Dutch national law called the CBW provides guidance on development of organizational policy on patch management under the obligation of 'Duty of Care' (Dutch: Zorgplicht). It emphasizes the importance of a change management policy that includes patch management (National Cyber Security Centre, 2023b). It mandates a structured change management process that includes risk assessment, prioritization, rollback procedures, and logging of changes. CBW also stresses the importance of timely patch installation, particularly for critical vulnerabilities and systems, and recommends testing patches in a controlled environment before deployment (National Cyber Security Centre, 2023b).

DORA which specifically targets financial entities, provides a detailed regulatory technical standard for ICT risk management, which includes a patch management component. It mandates the identification and classification of ICT-supported business functions, information assets, and ICT assets. This shows the need for organizations to have a thorough understanding of their IT ecosystem to inform patch management decisions. DORA emphasizes the identification of critical assets and their interdependencies, ensuring that patch prioritization aligns with business impact. Moreover, it requires the identification of processes dependent on third-party service providers to extend the scope of patch management to encompass the entire supply chain. DORA also mandates the maintenance of inventories of information and ICT assets to ensure that the activities related to patch management are based on accurate and up-to-date information.

Within DORA, procedures for vulnerability management are explicitly required, including the verification of third-parties handling vulnerabilities (European Banking Authority et al., 2022). This extends to tracking the usage of third-party libraries and ICT services and shows the need for version control and updates, especially for critical (business) functions. DORA also requires organizations to establish clear patch management procedures to ensure a structured and efficient approach to keeping systems secure (European Banking Authority et al., 2022). It emphasizes the use of automated tools to identify and assess patches to the extent possible (European Banking Authority et al., 2022). However, it isn't clear what is meant by the extent and how this is measured. The DORA act mandates emergency patching procedures in cases where critical vulnerabilities arise (European Banking Authority et al., 2022). Additionally, it requires organizations to set deadlines for the installation of software and hardware patches and updates (European Banking Authority et al., 2022). For the instances where such deadlines cannot be met, organizations must have escalation procedures established to handle any delays or complications effectively (European Banking Authority et al., 2022).

The BIR mentions the need for timely patch deployment in its guidelines, specially for vulnerabilities with a high likelihood of exploitation and significant impact (Dutch Central Government, 2018). It man-

dates organizations of the central government to have a process for managing technical vulnerabilities, including regular penetration testing, vulnerability risk analysis, and patch management (Dutch Central Government, 2018). Similarly, BIO, the successor of the BIR, emphasizes the timely acquisition of information on technical vulnerabilities, assessment of exposure, and implementation of appropriate mitigation measures for organizations across all layers of the Dutch government. It mandates for immediate patching of vulnerabilities with high exploitation likelihood and damage potential, and restricts software installation by users to prevent uncontrolled changes (Centre for Information Security and Privacy Protection, n.d.). Although, these practices are enforced, it isn't clear what 'immediate' action entails.

* Phase 1: Patch Information Retrieval

Standards on Phase 1
Mell et al. (2005) highlight the importance of having a clear patching and vulnerability management policy as the backbone of effective information retrieval. This policy should clearly define how the organization retrieves information on available patches and known vulnerabilities. A crucial part of this process is staying proactive, which requires organizations to regularly monitor security sources for patches, remediation strategies, and emerging threats that could affect the organization's systems. ISO/IEC (2013) stresses that staying up to date is key when dealing with security vulnerabilities. The sooner an organization learns about a new threat, the quicker it can assess its risk and take action. To achieve this, it's important for organizations to maintain a regularly updated list of trusted information sources for software that is relevant to them (ISO/IEC, 2013). Similarly, IEC (2015) stresses the importance of routinely checking for software updates and patches to keep systems secure. This helps ensure that the organization is always working with the most accurate and up-to-date information. By doing so, companies can stay ahead of potential risks and react swiftly when necessary.

It can also occur that no patch is available or an organization is unaware about an available patch for a known vulnerability. When it comes to identifying missing patches, Souppaya and Scarfone (2013) suggest that organizations carefully evaluate different techniques before deciding on an approach. Options like agent-based scanning, agentless scanning, and passive network monitoring each have their own advantages and disadvantages (Souppaya & Scarfone, 2013). Selecting the right method depends on the organization's needs, resources, and security goals.

Furthemore, relying on just one source of information isn't enough. Souppaya and Scarfone (2022) recommend tapping into a variety of sources, such as vulnerability feeds from software vendors, security researchers, and the National Vulnerability Database (NVD). (ISO/IEC, 2013) adds that joining industry groups and forums can also be valuable. These communities provide insights into best practices, security developments, early warnings, and expert advice while also encouraging knowledge sharing (ISO/IEC, 2022).

Lastly, considering that not only security threats, but also organizations' IT landscapes are constantly evolving, organizations need to keep improving their information retrieval processes. ISO/IEC (2022) advises regularly updating the list of information sources based on new findings or changes in the system inventory.

EU Policies and (Dutch) Guidelines on Phase 1
Not many EU regulations or Dutch guidelines specifically address the retrieval of information about patches and vulnerabilities. Most best practices in this area are based on international standards and industry recommendations rather than strict regulatory requirements.

However, the main regulatory framework addressing this topic is the DORA act, which applies to financial entities within the EU. DORA includes specific requirements related to monitoring and assessing vulnerabilities (European Union, 2022). The Regulatory Technical Standard for ICT Risk Management under the DORA ACT states that organizations must identify and update relevant and trustworthy information sources to maintain awareness of vulnerabilities (European Banking Authority et al., 2022). Furthermore, organizations must conduct automated vulnerability scans and assessments of their ICT

assets (European Banking Authority et al., 2022). The frequency and scope of these activities should align with the classification of assets (as outlined in Article 8(1) of Regulation (EU) 2022/2554 (European Union, 2022)) and the overall risk profile of the ICT asset (European Banking Authority et al., 2022).

* Phase 2: Vulnerabillity Scanning, Assessment and Prioritization

Standards on Phase 2
SSPM also involves vulnerability scanning, risk assessment, and prioritizing security patches before the respective vulnerabilities can be exploited. In this phase, the first step is vulnerability scanning, which helps detect weaknesses in an organization's IT systems, applications, and networks based on the retrieved information about patches and vulnerabilities in Phase 1. ISO/IEC (2022) stresses the importance of using scanning tools suited to the organization's specific technologies. Automated scanning is a great starting point, but it isn't foolproof (ISO/IEC, 2013). That's why it should be complemented with regular penetration tests and vulnerability assessments, which provide a deeper look into potential security gaps.

However, identifying vulnerabilities is merely the first step. Souppaya and Scarfone (2013) emphasize that before deploying patches, organizations must also validate patches' authenticity and integrity. This ensures that patches haven't been tampered with or compromised, which reduces the risk of introducing malware or causing unexpected system failures.

Additionally, not all vulnerabilities pose the same level of threat, so organizations need to assess which ones matter most. According to ISO/IEC (2022), this means carefully reviewing reports to determine the actual impact of each vulnerability and deciding on the best course of action, whether that's updating software, applying security controls, or taking other measures to reduce the risk (ISO/IEC, 2022).

(Souppaya & Scarfone, 2022) take this a step further and highlight key factors to consider when assessing vulnerabilities. A key factor is the likelihood of exploitation, meaning how easy and likely it is for attackers to take advantage of this vulnerability. Another factor is the negative impact on systems, meaning in the case a vulnerability is exploited, what could happen and to what extent does the impact manifest itself? Could it lead to data loss, system downtime, or reputational damage? Moreover, a factor to consider is the alternatives to patching if patches are unavailable or patching is not possible. Are there alternative ways to reduce the risk, such as temporary security controls or configuration changes? Lastly, it's also important to consider the impact on business operations as some patches might require downtime, so scheduling them strategically is key.

Since organizations often deal with hundreds or even thousands of vulnerabilities, fixing everything at once isn't practical. Therefore, Mell and Tracy (2002) and Mell et al. (2005) emphasize the need for a defined procedure with outlined criteria to prioritize patching and determine which systems and patches are addressed first. This highlights the importance of not treating all vulnerabilities equally and adopting a risk-based approach. ISO/IEC (2013, 2022) recommends focusing on the most critical vulnerabilities first—those that pose the greatest risk to business operations. Similar to what Souppaya and Scarfone (2022) recommended, it is recommended to address high-risk systems first given the principle of focusing on vulnerabilities with the greatest potential impact (ISO/IEC, 2013, 2022). ISO/IEC (2013) also suggests that the urgency of addressing a vulnerability should dictate the speed of the response which potentially triggers change management or incident response procedures. ISO/IEC (2013) stresses the importance of aligning vulnerability management with incident management activities and communicating vulnerability data to the incident response function. This ensures a coordinated and effective response to security incidents (ISO/IEC, 2013).

During this phase organizations should also keep in mind that the ISO/IEC (2022) stress the importance of setting clear timelines for patching and mitigation. IEC (2015) recommends scheduling authorized, effective patches based on system design and operational constraints. It also emphasizes the importance of maintaining accurate records of installed, authorized, and released software versions and regularly determining compatible upgrades and updates (IEC, 2015).

EU Policies and (Dutch) Guidelines on Phase 2
NIS2 establishes that enhancing cybersecurity resilience begins with a thorough risk analysis. The NIS2 directive is transposed into the Dutch national law called 'Cyberbeveiligingswet' (CBW). The CBW also emphasizes risk analysis as the initial step for gaining essential insights into an organization's security posture. This perspective shows that understanding the potential threats and their impact is paramount before any patching is done or remediation efforts are undertaken.

Building upon this, the DORA act introduces a regulatory mandate for automated vulnerability scanning and assessments, particularly within the financial sector (European Union, 2022). The frequency and scope of vulnerability scans should match how critical an organization's ICT assets are and the level of risk they carry (European Banking Authority et al., 2022). This act dictates that the frequency and scope of vulnerability scanning and assessments, which directly inform patch deployment, must be proportional to the criticality and risk profile of the ICT assets. DORA further stresses the need for regular risk assessments, especially when making significant changes to network infrastructure or dealing with legacy systems (European Banking Authority et al., 2022). This shows the growing shift towards a more proactive approach rather than reactive, where continuous monitoring and automated detection are used.

The DORA act also shows the need to prioritize patch deployment based on how critical a vulnerability is, the classification of the affected asset, and its overall risk profile (European Banking Authority et al., 2022). A risk-based approach is assumed to ensure that organizations use their resources efficiently and that the most serious threats are addressed first.

Similarly, Dutch Central Government (2018) emphasizes the value of risk assessment when applying patches. It recommends weighing the risks of the vulnerability against the potential risks of installing the patch, as some updates may introduce instability or compatibility issues (Dutch Central Government, 2018). Additionally, BIR advises organizations to keep scan reports as a way to track changes over time and spot potential security gaps (Dutch Central Government, 2018).

* Phase 3: Patch Testing

Standards on Phase 3
One of the most crucial aspects of SSPM is ensuring that software patches are tested thoroughly before they are deployed in live environments. Mell and Tracy (2002) laid the groundwork for this approach and advocated for a well-defined patching policy that includes a structured methodology for testing and safely applying patches. Testing should consider usability, security and effects on other systems, and userfriendliness (ISO/IEC, 2013). Mell et al. (2005) further recommended that patches and alternative remediation methods should be tested in standardized environments that mirror real-world deployments. This ensures that organizations can confidently apply updates without introducing new problems. For industrial systems, the risks of patching are even higher. Later, the (IEC, 2015) similarly recommended that patches should be tested in controlled environments that accurately reflect production setups. This is crucial to ensure that updates do not compromise system reliability or operational functionality. ISO/IEC (2022) extends this by emphasizing the need to use segregated environments for testing ICT components to avoid unintended disruptions in live systems, and to keep development and testing environments patched and up to date to maintain security even in non-production setups.

ISO/IEC (2013) highlights the risks of applying patches without thorough testing. While software vendors work to release patches quickly, time constraints mean that some updates may contain flaws. This makes independent testing essential to verify effectiveness and identify potential side effects before rolling out updates organization-wide (ISO/IEC, 2013). If immediate patching isn't an option, (ISO/IEC, 2013) suggests alternative security measures, such as disabling vulnerable services or tightening access controls, to reduce exposure to threats.

Another practical challenge is the availability of resources for patch testing. Not every organization has the capacity to conduct extensive testing in-house, which is why ISO/IEC (2013) and ISO/IEC

(2022) suggest delaying patch installation in certain cases. This gives time to monitor issues reported by other users before applying updates.

Souppaya and Scarfone (2013) highlight the complexities of patch management, emphasizing the need to identify and resolve conflicts that may arise when different patches interact. The importance of detecting unexpected side effects, such as changes to security settings, that could introduce new vulnerabilities rather than fixing old ones is alos stressed upon (ISO/IEC, 2013, 2022; Souppaya & Scarfone, 2013, 2022).

EU Policies and (Dutch) Guidelines on Phase 3
While the NIS2 Directive does not explicitly include patch testing as a detail, this directive and its transposition into CBW inherently require organizations to have policies and procedures to assess the effectiveness of cybersecurity risk-management measures (European Parliament, 2022). This may involve establishing policies and procedures for testing the effectiveness of patches, implying that organizations should not only implement patches but also verify their efficacy in mitigating known vulnerabilities. The DORA act, on the other hand, directly addresses patch management and requires entities to ”test and deploy the software and hardware patches and the updates (European Banking Authority et al., 2022).”

* Phase 4: Patch Deployment

Standards on Phase 4
Effective patch deployment starts with a clear policy and structured methodology. (Mell & Tracy, 2002) emphasize that patching should be a well-planned process that includes both testing and safe installation. Mell et al. (2005) advocate for automated patch deployment using enterprise patch management tools. Where feasible, they recommend automatic updates, reducing the need for manual intervention and streamlining the patching process. However, not all patches can or should be applied immediately across an entire system (Souppaya & Scarfone, 2022). Automation plays a key role in modern patch management, but ISO/IEC (2022) emphasizes that organizations must find the right balance. Souppaya and Scarfone (2022) note that factors such as software type, platform, and operational constraints all influence how updates should be distributed. Therefore, they introduce the concept of phased deployment, which allows patches to be installed on a small subset of systems—often called ”canary” assets—before rolling them out organization-wide. While automation can speed up patch deployment and reduce human error, there are situations—such as updates affecting critical business operations and where manual oversight is necessary (ISO/IEC, 2022). In these cases, a controlled rollout with careful monitoring is the best approach (ISO/IEC, 2022). This approach helps detect potential compatibility or security issues early and reduces the risk of widespread failures. That is why, while automation improves efficiency, it’s equally important to have control measures in place.

Additionally, they highlight the importance of a centralized log to track updates, monitor progress, and maintain an overview of the deployment and statuses of patches. ISO/IEC (2013) stresses that only authorized personnel should execute updates and that all changes should be carefully logged for accountability and traceability. This prevents unauthorized modifications and ensures a clear record of all patching activities.

From a technical perspective, Souppaya and Scarfone (2013) take resource constraints into consideration and mention the need for patch management solutions that don’t overload system resources. It is also recommended to prevent users from interfering with patching processes to ensure that updates are applied consistently across the organization (Souppaya & Scarfone, 2013). Additionally, they advocate for continuous monitoring to quickly identify and resolve any issues that arise post-deployment (Souppaya & Scarfone, 2013).

EU Policies and (Dutch) Guidelines on Phase 4
DORA mandates the ”test and deploy” of software and hardware patches (European Banking Authority et al., 2022). Furthermore, the DORA act emphasizes the prioritization of patch deployment based on the identified vulnerabilities to make sure that critical vulnerabilities are addressed in a timely manner

(European Banking Authority et al., 2022).

On the other hand, Dutch guidelines such as the BIR (Dutch Central Government, 2018) focuses on the deployment of patches within technical infrastructures and advocates for verification of the latest updates, preferably through automation. However, it also acknowledges the need for control and that automatic patch deployment should only occur with specific agreements from the software vendor.

* Phase 5: Post-Deployment Patch Verification

Standards on Phase 5
Mell et al. (2005) mention that remediations should be verified through network and host vulnerability scanning to ensure that vulnerabilities have been properly addressed. ISO/IEC (2013) takes this further by requiring regular evaluations of the vulnerability management process. This means organizations must not only check whether patches are installed but also assess whether they are working as expected. Souppaya and Scarfone (2022) and the ISO/IEC (2022) stress the need for continuous monitoring of patched software behavior, particularly to detect potential security issues or unintended changes. They also highlight the risk of patched systems being unknowingly deactivated or compromised. In this case, verification should go beyond simply checking if a patch was applied, it must also assess its effectiveness and detect any side effects. Souppaya and Scarfone (2013) and the ISO/IEC (2022) recommend using independent vulnerability scanners instead of relying solely on the patch management system to conduct a more objective and accurate verification.

Maintaining detailed records of updates and system changes is essential for accountability and troubleshooting. The IEC (2015) recommends keeping quarterly records of all installed, authorized, and released software versions, helping organizations track patch history and ensure compliance. The ISO/IEC (2013) also advocates for archiving previous software versions, including all relevant parameters and configurations. (ISO/IEC, 2022) stresses the need for maintaining audit logs and ensuring that updates are properly documented and monitored to maintain visibility and control. This makes it easier to restore systems if a patch causes unexpected issues. Even with thorough testing, patches can sometimes cause operational disruptions or unexpected side effects. To mitigate this, rollback strategies, a plan to quickly revert to a stable system state, are emphasized (ISO/IEC, 2022; Souppaya & Scarfone, 2022). Automation can be used in this case (Souppaya & Scarfone, 2022).

EU Policies and (Dutch) Guidelines on Phase 5
There are no specific regulatory requirements that explicitly mandate patch verification. However, the DORA act does emphasize broader vulnerability remediation and monitoring. It mentions that ”Organizations must monitor and verify the remediation of vulnerabilities” (European Banking Authority et al., 2022) to ensure that security vulnerabilities are effectively addressed by organizations. Furthermore, there is a requirement to record detected vulnerabilities affecting ICT systems and track their resolution over time (European Banking Authority et al., 2022).

2.4. Conclusion of Reviewed Regulations

All of the reviewed regulations share the goal of improving cybersecurity by ensuring organizations proactively manage software vulnerabilities. Each mandates that organizations have formal patch management processes in place and treat timely patching of critical flaws as a priority for cyber defense and resilience. In every case, patch management is recognized as a cornerstone of risk mitigation against known threats, whether explicitly (as in BIO’s one-week rule or DORA’s requirements) or implicitly as part of general security duties (as in NIS2’s cyber hygiene requirements). Across the regulations, organizations are expected to monitor for relevant vulnerabilities, apply security patches or mitigations in a timely manner, and integrate patching into their security program.

Despite their common emphasis on patching, these regulations differ in scope and in how they define obligations, enforcement, roles, and timelines. Each regulation targets different domains. BIO (and its predecessor BIR) apply to Dutch public-sector institutions, which establishes baseline security controls for Dutch government agencies. DORA, by contrast, is tailored to EU’s financial sector, which

covers banks, insurers, and other financial entities EU-wide. NIS2 Directive has the broadest scope, which spands multiple critical sectors and key digital service providers across all EU member states. This means an organization's obligations may vary depending on which legislation it falls under (e.g. a Dutch ministry vs. a private bank vs. an energy utility). Some organizations might fall under multiple legislation.

Furthermore, the regulations vary from prescriptive to principle-based. BIO is quite prescriptive and explicitly requires patches for critical vulnerabilities to be applied within a set timeframe. It directly specifies what must be done and how quickly and leaves little ambiguity for those under its mandate. DORA also introduces detailed obligations via its technical standards. It requires specific actions like maintaining asset inventories, conducting risk-based patch prioritization, and setting internal patch deadlines. However, DORA's approach is risk-driven. It does not dictate one universal patch deadline for all organizations, but it forces organizations to define procedures that ensure patches are deployed timely relative to the risk criticality. In contrast, NIS2 is more high-level. It mandates "appropriate and proportionate" security measures, which implies organizations should institute patch management policies, but it does not stipulate explicit patching timelines or detailed processes either. The burden is on companies to interpret what timely patching means in their context to meet NIS2's general requirements. In summary, BIO (and analogous mandates like the US's CISA KEV deadline) mention exact expectations, whereas NIS2 relies on broader principles of due care, and DORA lies somewhat in between.

Another clear practical difference is how patching speed is addressed. BIO sets a firm deadline, e.g. one week for top-priority patches, which creates a sense of urgency. NIS2 does not give any fixed timeline, simply expecting patches to be applied "in a timely manner" as part of risk management. This can lead to ambiguity, as organizations must judge what constitutes an acceptable delay. DORA and NIS2 require timely patching too. Organizations must define and adhere to their own patch deployment timeframes and have emergency procedures for urgent fixes. All frameworks do agree that critical vulnerabilities shouldn't be left unaddressed for long, but the explicitness of the mandate varies greatly.

Lasltly, as an internal government standard, BIO compliance is enforced via government audits and IT governance processes, rather than fines. Its impact is mainly within public administration, and it sets a benchmark that the government also encourages private organizations to follow voluntarily. NIS2 and DORA, on the other hand, are backed by law across Europe with designated supervisors and regulators. Under NIS2, national CERTs will monitor compliance, and organizations that fall short can face administrative fines or other sanctions. The directive even allows penalties on individuals. In extreme cases, executives can be held liable for major security breaches. DORA similarly empowers financial regulators (such as central banks) to enforce its requirements with inspections and penalties for institutions that do not meet the ICT risk management standards. In summary, non-compliance with NIS2 or DORA can result in significant legal and financial consequences, whereas BIO's enforcement is more about meeting mandated best practices within the public sector.

3

Research Gap & Objectives

3.1. Research Gap

3.1.1. Existing Knowledge

Research on patch management has primarily focused on the human, technical and organizational dimensions. From a technical standpoint, studies have examined the complexities of patch deployment, including risks such as software incompatibility, deployment failures, and security gaps due to unpatched vulnerabilities (Cavusoglu et al., 2006; Dissanayake et al., 2021). From a human perspective, research has explored the role of sysadmins in decision-making, by for example emphasizing their reliance on experience, peer networks, and fragmented information sources when applying patches (Jenkins et al., 2024; F. Li et al., 2019). Studies have also highlighted issues such as cognitive overload, lack of situational awareness, and the tendency to delay patching due to uncertainty about stability or operational impact (Barrett, 2004; Beattie et al., 2002; Hrebec & Stiber, 2001). On an organizational level, research has shown that patch management is shaped by internal policies, security culture, and business priorities (Dissanayake, Zahedi, et al., 2022; Shostack, 2003). Given organizations need to handle large volumes of patches, a prioritization model has also been proposed (Zhu et al., 2011). Though, the approach to such models is limited to the initial decision-making phase and does not address critical aspects such as stakeholder communication, involvement of higher management, or the broader organizational impact of patching decisions. To address this, Gentile and Serio (2019) made an attempt at surveying standards for industrial control systems and provided a workflow of patch management processes. This workflow provides insight into the decision-making and sub-processes of patch management process involving system owners, industrial control system developers, and management. In relation to this, studies have found that organizations often struggle with structured vulnerability assessment, and balancing security against operational continuity (De Smale et al., 2023; Kraemer & Carayon, 2007). Yet, organizations still continue to struggle with balancing security and operational stability (Andrew, 2005; Dissanayake, Jayatilaka, et al., 2022b).

More recently, it was observed that patching practices are increasingly influenced by regulations and mandates by governments. From a regulatory perspective, a study by ten Napel et al. (2024) provides one of the first empirical analyses of regulatory patching deadlines at a Dutch public sector organizations under the BIO framework. By analyzing ticketing data and conducting interviews, ten Napel et al. (2024) show that while the one-week mandated patching deadline is often missed, it still triggers escalated responses and managerial attention. This study showed how regulatory pressure can accelerate remediation of vulnerabilities(ten Napel et al., 2024).

3.1.2. Knowledge Gap & Limitations of Current Research

Although previous studies have advanced the understanding patch management processes and challenges involved, they lack in several ways. Previous work, such as the one by Dissanayake, Jayatilaka, et al. (2022b), has mainly focused on organizations in the healthcare sector. While prior research has extensively examined the influence of organizational policies, security culture, and business priorities,

and often attribute decision-making authority to sysadmins, the growing role of EU's regulatory requirements has been overlooked. In contrast to previous work, such as Dissanayake, Jayatilaka, et al. (2022b) and Jenkins et al. (2024), ten Napel et al. (2024) found that sysadmins do not solely appear to have the authority to plan patching according to their own design, but are rather influenced by external pressure of the BIO regulation.

With the increasing regulatory pressure introduced by EU policies such as the NIS2 Directive and the DORA Act, as well as Dutch national legislation like CBW and guidelines such as the BIO, organizations in other sectors (e.g. financial sector) could also no longer solely be shaping their patch management policies and practices based on internal priorities. Instead, external regulations are imposing new requirements and expectations on both sysadmins and organizations. Despite this, more recent research, such as the study by ten Napel et al. (2024), only account for Dutch BIO framework and fail to account for more recent and higher-level EU regulations.

In this regard, the first gap that arises is wether such high-level and abstract EU legislation leads to a faster patching speed and frequency, or whether delays are caused by its requirements. There is a lack of clarity on how organizations translate non-prescriptive legislation like DORA and NIS2 into concrete patching policies and procedures and what challenges they face when doing so. Moreover, it is unclear how the previously mentioned socio-technical factors interact with new requirements mandated by EU legislation.

Lastly, current understandings of patching processes fail to provide a structured workflow that fully integrates regulatory requirements (European Parliament (2022) and European Union (2022)). Previous patching workflows, such as the one presented by Gentile and Serio (2019), mainly lack detail on the different stakeholder roles, speeding or accountability mechanisms, and reporting structures under regulatory pressure. Gentile and Serio (2019) do not systematically address all stakeholders, challenges and phases of patch management processes. For example, the challenges of communication and coordination between coordinators, SOC's, and a national CERT are overlooked (Dissanayake, Zahedi, et al., 2022), and little attention has been paid to the specific phases of patch management, such as patch information retrieval and patch deployment (Dissanayake, Jayatilaka, et al., 2022b).

Incorporating these regulatory influences would therefore be beneficial. Aside from regulations, key stakeholders have not been integrated into a structured workflow. Sectors other than industrial control systems that are regulated by EU legislation can benefit from an improved workflow for a better understanding of patching under regulations.

3.1.3. Novelty & Research Aim

Building on previous research, this study aims to take a holistic approach to patch management by accounting for technical, human, and organizational, and regulatory factors. Therefore, this study can generate new knowledge and elaborate on socio-technical factors in patch management under regulatory pressure. Furthermore, this study will look at what challenges organizations now face when translating new mandates into patch management policies and processes. It also looks at how patching speed and frequency, and documentation and reporting differs under non-prescriptive EU regulations (compared to the BIO regulation).

Lastly, this research aims to improve the patching process model by studying how and where current EU regulatory requirements, and mechanisms that directly enforce speed (compared to BIO), impact different sub-processes of patch management. A structured workflow for the patch management process can be developed by mapping the involved stakeholders, their roles and responsibilities, and the different phases and the associated sub-processes of patch management. Each phase presents unique barriers, which are influenced by various socio-technical factors, including regulatory, human, organizational, and technical influences.

3.2. Research Questions

Consequently, this thesis aims to understand how organizations operationalize patch management under recent EU regulations such as NIS2 and DORA, and how the absence of mandated timelines affects their timeliness and ability to respond to vulnerabilities. It further seeks to explore the challenges and barriers that arise for patch management caused by such regulatory pressure. The insights will then be examined in relation to the socio-technical factors that influence patch management processes.

How do regulations influence organizations' patch management policies and practices, and how do socio-technical factors interact with these?

The main research question can be decomposed into several sub-research questions (SRQs):

- SRQ1: What are the challenges organizations face when translating regulations such as BIO, DORA and NIS2 into patch management policies, standards and practices?
- SRQ2: How have patching speed, and documentation and reporting changed since the introduction of regulations?
- SRQ3: What roles and responsibilities, and sub-processes form an organization's patch management workflow under regulations?
- SRQ4: What role do socio-technical factors continue to play in the patch management process/-workflow?

Existing literature looks at patching under regulatory deadlines, yet largely overlooks the nuanced challenges and complexities that arise when translating non-prescriptive EU cybersecurity regulations like NIS2 and DORA into internal organizational practices. It is unclear what challenges organizations face regarding background processes or prerequisite activities that influence the effective and timely implementation of patch management under regulatory requirements. Furthermore, it is unclear how organizations translate such regulations into their internal vulnerability and patch management policies. SRQ1 explores how organizations interpret and implement regulations into concrete patch management policies, processes and standards and what challenges arise.

Current research only predominantly focuses on patching speed under the BIO regulation. It is unclear how regulations, that do not prescribe a deadline, affect patching speed and documentation practices. SRQ2 tries to understand whether and how EU regulations practically accelerate patching speed or inadvertently slow down processes and the factors that might play a role in doing so, such as increased documentation, reporting requirements, or bureaucratic overhead.

SRQ3 aims to identify the key stakeholders and processes involved in patching and understand the roles and responsibilities within large organizations. This is crucial for identifying how patch management responsibilities are allocated to develop a socio-technical workflow for patch management. In many organizations, the patch management process involves various stakeholders, including sysadmins, system/asset owners, security teams, and compliance officers, and different sub-processes such as retrieval of patch information, patch deployment, etc.

Lastly, by investigating the specific impact of these regulations in relation to socio-technical factors on stakeholders' decision-making, processes and practices, SRQ4 aims to understand how regulations influence the day-to-day activities of patching. While the literature recognizes socio-technical factors influencing patch management, few studies explicitly examine how these socio-technical dimensions continue to evolve or persist under the pressures exerted by recent regulatory frameworks like NIS2, DORA, and BIO. SRQ4 explicitly examines socio-technical factors in patch management under current regulatory conditions, and explores how regulation may mitigate, reinforce, or introduce new socio-technical frictions and challenges. It looks at potential barriers organizations are facing in relation to regulations, but also at how these regulations can enable organizations to work around such barriers.

3.3. Implications

From a scientific point of view, this research deepens our understanding of patch management practices in large organizations, particularly in the context of evolving regulations. It fills a gap in existing literature by examining how regulatory requirements such as NIS2, CBW, and DORA influence both organizational policies and the actual implementation of patch management. The socio-technical approach, integrating technical, human, and organizational factors into a workflow gives insight into the process and complexities of patching. The findings can inform future studies on improving patching workflows, and compliance strategies.

From a societal perspective, this research is particularly important because it addresses the increasing regulatory pressure on and the need for better patch management processes. The insights from this study offer practical advice to organizations help improve security, reduce the risk of exploitation of vulnerabilities, and ensure organizations stay compliant with regulations. It can also inform policymakers about potential gaps in current legislation.

4

Methodology

4.1. Semi-structured Interviews

To gain an in-depth understanding of how organizations interpret and implement patch management practices under DORA and NIS2, a series of semi-structured interviews was conducted with cybersecurity professionals from both a consultancy firm and two client organizations. An overview of the participants can be found in Table 3. These interviews focused on discovering how organizations manage patching in the absence of strict deadlines, and how regulations are operationalized in different settings.

The interviews were held with participants involved in different aspects of patch management, including security operations, IT infrastructure, risk and compliance, and consulting. The aim was to triangulate perspectives across technical, governance, and advisory roles. Semi-structured interviews were chosen as the primary method for qualitative data collection due to their ability to balance structure with flexibility. Structured interviews allow for direct clarification of specific topics but often lack depth, while unstructured interviews can yield rich insights but are time-consuming and harder to steer. Semi-structured interviews provide a balance by allowing the interviewer to follow a prepared set of questions, while still enabling the addition or omission of questions based on the flow of conversation. This flexibility was essential for exploring complex decision-making processes and getting role-specific nuances.

The initial questions were informed by the literature review and preliminary discussions conducted at the selected case study organizations. These prior steps helped personalize the interview guides to reflect the organization context, the role of the interviewee, and current patch management processes and regulatory pressures.

Table 3: Overview of participants, their roles, industry sectors, experience, and key responsibilities.

ID	Participant Role	Industry/Sector	Years of Experience	Work Experience & Duties
P01	Analyst	Financial Services	2	Implementation DORA updates to Patch Management policies and standards. DORA workshops between key stakeholders in patch management.
P02	Analyst	Financial Services	2	Implementation DORA changes in Vulnerability Management Standards & Policies and Incident Management & Reporting for Financial Entity.
P03	Consultant	Financial Services, IT/Operational Technology	4	Responsible for DORA Capabilities; DORA Policy Gap-Assessment; Translation of DORA to policies and processes; Previously, factory and Proof of Concepts (POCs)-related topics in Operational Technology.
P04	Associate Director	IT/Operational Technology	20	Communications, Media & Technology Industry Lead; Managing Industry Relations; Technical & Operational experience.
P05	Analyst	IT/Operational Technology	3	Responsible for operational vulnerability management; Functional contact and coordinator between identified CVEs and affected system/asset owners. Previously a Security Operations Center (SOC) analyst.

Continued on next page

Table 3 – continued from previous page

ID	Participant Role	Industry/Sector	Years of Experience	Work Experience & Duties
P06	Consultant	Public Services (government)	3	Responsible for Hybrid Multi-Cloud implementation at government; Implement BIO security controls on architecture and compliance level; Cloud Security and Cloud Sovereignty.
P07	Manager	Public Services, Financial Services	13	Vulnerability Management under BIO for government; Vulnerability Management under DORA for financial entity.
P08	Senior Manager	Financial Services	15	Financial Services Industry Lead; Managing Industry Relations; Quality Assurance.
P09	Associate Manager	Public Services (government)	6	Responsible for NIS2 Capabilities; Focus on governance of security in Health & Public Services (H&PS) and (national) regulations such as BIO and NIS2. Previously did SOC advisory, vulnerability management, monitoring, reporting, and Identity & Access Management.
P10	Product Owner Security Assurance	Financial Services	25	Product owner for different CISO services including anti-malware, data loss prevention, cloud app usage, and also NTDs measures; Security Assurance including vulnerability management, hardening and offensive security (penetration testing and red teaming).
P11	IT Process Improvement Specialist	IT/Operational Technology	5	Vulnerability Management Process Owner at IT/OT manufacturer
P12	Senior Manager	Financial Services	10	Responsible for Vulnerability Management and Incident Response under DORA at several financial entities
Total: 12			Average: ± 9	

4.1.1. Selection of Case Studies

Consultants

This research is conducted as part of a master's internship at a consultancy firm, Accenture, that supports a range of clients in both the private and public sectors with cybersecurity-related questions. Accenture provides expertise in various areas, among which vulnerability management, compliance readiness, security patching, and the implementation of recent EU legislation, including the Digital Operational Resilience Act (DORA) and the Network and Information Security Directive (NIS2). Accenture consultants provide both strategic and operational cybersecurity work and support their clients in interpreting and applying regulatory requirements in their security and IT environments. The first organization for this study will be Accenture.

As part of this study, two clients of Accenture have been selected to serve as case studies. These clients represent contrasting sectors and fall under different EU regulatory regimes, which provides a unique opportunity to conduct a cross-regulatory comparison of how patch management processes are shaped by EU legislation.

Case 1

The financial services sector remains one of the most high-risk environments when it comes to cybersecurity threats, with data breaches often resulting in significant financial costs, reputational damage, and legal consequences. An example of the importance of timely patching in the financial services sector is the Equifax data breach, which occurred in September 2017 and affected approximately 147 million customers (Goodin, 2017). The breach was caused by the exploitation of a known vulnerability in the Apache Struts web application framework (Goodin, 2017). Despite a patch for this vulnerability being available for over six months, Equifax had failed to apply it in time. This allowed attackers to gain initial access through a public-facing web portal and move laterally across unsegmented internal systems (Kost, 2025). Once inside, attackers found plaintext credentials and used them to escalate privileges (Kost, 2025). This way the attackers were able to maintain undetected access for months due to an expired encryption certificate on a key monitoring tool (Kost, 2025).

The compromised data included highly sensitive personally identifiable information (PII) such as names, dates of birth, Social Security numbers, driver's license numbers, and credit card information (Kost, 2025). The consequences were severe. Equifax faced public backlash, accusations of insider trading, and ultimately a $700 million regulatory fine (Kost, 2025). This case shows the critical importance of

timely remediation of vulnerabilities. It also shows how unpatched vulnerabilities can lead to systemic breaches with widespread societal and economic impact.

Including a financial institution subject to DORA as a case study in this research is therefore highly relevant. Financial organizations in the EU, and specifically in the Netherlands, are required under DORA to demonstrate robust ICT risk management practices, including effective patch management. Financial institutions are required under DORA to implement and continuously improve ICT risk management practices, including patch and vulnerability management. While DORA does not prescribe strict patching deadlines, it does emphasize proportionality, accountability, and the need for documented, defensible security practices. The Equifax breach is an example of the real-world risks of failing to implement timely and effective patches, which is the kind of challenges this study aims to explore.

Therefore, the first client organization is a bank operating in the financial services sector, subject to the provisions of DORA. The bank provides a complex but mature IT environment with dedicated risk, compliance, and security teams. Its regulatory exposure and systemic importance to the EU financial system nature make it a compelling case for examining how organizations under DORA approach patch management.

Case 2
Recently, there has been a series of high-profile incidents that revealed critical vulnerabilities in industrial systems. One of the earliest wake-up calls was the Stuxnet worm attack, which in 2010 targeted supervisory control and data acquisition (SCADA) systems and demonstrated how malware could disrupt physical industrial processes (Chen & Abu-Nimeh, 2011; Gentile & Serio, 2019; Karnouskos, 2011). This event raised awareness on cyber risks in OT environments, specially those based on proprietary protocols and legacy infrastructure. More recently, widespread hardware-level vulnerabilities such as Meltdown and Spectre forced many industrial control system (ICS) vendors to initiate urgent patching campaigns (Gentile & Serio, 2019). Although these vulnerabilities pertained to hardware, the rushed deployment of patches had unintended consequences. Several vendors and users reported that the fixes significantly degraded system performance (Gentile & Serio, 2019). This still shows the trade-offs and complexities of patching in industrial and OT environments.

Including a high-tech IT/OT company is relevant because the organization's environment spans both IT and OT (Operational Technology) domains which adds layers of complexity to vulnerability and patch management. OT systems often have stricter uptime requirements and are harder to patch without disrupting operations.

At present, the IT/OT organization must adhere to the NIS2 Directive, which is designed to strengthen the EU's and Netherlands' digital resilience. Due to the essential role this company plays in technology supply chains and its use of critical infrastructure, it falls under the scope of NIS2. Under this legislation, Providers of Essential Services are required to implement measures that protect their information and communication systems against cyber threats. They are also obligated to report any serious cyber incidents to the appropriate authorities.

4.1.2. Recruitment of Participants

This research used convenience sampling to select participants for the semi-structured interviews. Convenience sampling is commonly applied in qualitative research when participants are selected based on their accessibility and willingness to participate (Etikan et al., 2016). It is useful when the researcher has limited access to a full sampling frame or when the study aims to gain exploratory insights into specific experiences or processes (Etikan et al., 2016).

According to Yin (2003), selecting participants who are key actors within the organization ensures access to valuable perspectives supported by the participant's direct experience and understanding of patching processes or regulations. In this case, participants were selected based on their responsibilities and relevance to the research topic, and their availability through the researcher's existing professional network. As the researcher conducted this study within a consultancy firm, consultants

who regularly advise clients on NIS2 and DORA compliance were recruited. These consultants also acted as contact liaisons to client organizations and helped identifying and facilitating interviews with relevant internal stakeholders at the two case study organizations.

The selected participants included:

This sampling approach allowed for access to key informants who could speak directly to the research topic. It also aligned with the goal of gathering in-depth, role-specific perspectives on how patch management is understood and practiced in response to recent EU regulations.

While convenience sampling can limit the generalizability of findings and introduce selection bias, it was considered appropriate for this exploratory qualitative study, where the aim is not to produce statistically representative results but to generate rich, context-specific insights. The approach also supports the development of hypotheses and research directions for further investigation.

4.1.3. Interview Protocol

To explore how organizations approach security patching in the context of EU regulations such as DORA and NIS2, a semi-structured interview protocol was developed. This protocol was used as a guide for conducting in-depth interviews with participants. The questions were designed to be flexible and allowed for follow-up questions and probes depending on the participant's responses.

The interview guide was structured around key themes which were aligned with the research objectives and sub-questions. The semi-structured natured provided consistency between the interviews while also leaving space for rich and context-specific perspectives.The interview started with an introduction that aimed to gather background information about the participant's role and experience related to security patching. It included questions about their current position, tenure at the organization, and the extent to which their responsibilities involved vulnerability management and patching.

After, participants were asked about how patching policies are defined and operationalized within the organization. This included questions on how vulnerabilities are assessed and categorized, how internal timelines for patching are determined, and whether best practices or regulatory standards (such as ISO27002 or CISA KEV timelines) are used to base decisions on. The aim was to understand whether formal frameworks exist and how patching priorities are established, specially in cases involving high or emergency severity. Later, the interview was directed towards how participants stay informed about new vulnerabilities. Questions focused on the use of trusted sources, automated tools, or external advisories to maintain awareness continuously. The goal was to identify gaps or strengths in the information retrieval phase of patch management.

To assess the influence of regulatory frameworks, participants were asked how DORA and NIS2 had affected their organization's patching practices. This included probing for any changes in policies or workflows since the introduction of these regulations, and how these frameworks are interpreted internally. Special attention was given to how organizations handle ambiguous requirements, such as the absence of fixed patching deadlines.

After this, another section looked at internal and external factors that affect how quickly patches are applied. Participants were asked to identify organizational, technical, and regulatory barriers to timely patching. They were also asked whether regulatory expectations, such as documentation or reporting, contribute to delays, and whether their patching pace has changed due to regulatory pressure. Another key area which was focused on was how organizations handle high-severity or emergency vulnerabilities. Interviewees were asked about escalation protocols, criteria for declaring emergencies, and how patching exceptions are documented or risk-compensated. Probes were used to determine how these decisions align with or are influenced by legislation, especially in the absence of explicit patching deadlines. To conclude the interviews, participants were asked to reflect on trends in patch management, their perception of developments regarding legislation, and any future changes being planned in anticipation of audits or changes in regulatory expectations. The goal was to collect both evaluative and forward-looking insights.

Each interview lasted approximately 45–60 minutes and was conducted in either English, depending on the participant's preference. All interviews were recorded with consent and transcribed for subsequent analysis. The full interview protocols can be found in Appendix C.

4.2. Analysis and Presentation of Qualitative Data

To analyze the semi-structured interview data collected in this study, a reflexive thematic analysis approach was applied. The widely recognized TA framework developed by Braun and Clarke (2006) was followed. The interviews were designed to elicit open-ended responses around participants' roles, patching practices, prioritization methods, patch policy and standard development, and interactions with regulatory expectations. Thematic analysis allows for the identification of patterns, meanings, and insights across qualitative data and is particularly suited for exploring complex socio-technical processes such as those involved in patch management under evolving regulatory requirements.

This method was selected due to its flexibility and its ability to capture both inductive themes which emerged organically from the data. Reflexive thematic analysis embraces the researcher's active role in interpreting meaning from the data and allows the themes to be shaped iteratively as understanding deepens during the analysis process. ten Napel et al. (2024) successfully used Thematic Analysis in similar research, which shows the potential of it for this study.

The analysis followed the six phases proposed by Braun and Clarke (2006):

1. Familiarization: All interviews were transcribed and read multiple times to ensure a deep understanding of the data. Initial impressions and potential points of interest were noted.
2. Generating Initial Codes: Relevant features across the data set were systematically coded. These codes captured segments related to regulatory interpretation, decision-making in patching workflows, organizational dynamics, and perceptions of compliance.
3. Searching for Themes: Codes were then organized into broader themes that reflected recurring patterns, challenges, or strategies reported by participants.
4. Reviewing Themes: Themes were reviewed for coherence in relation to both the coded extracts and the data set as a whole. Where necessary, themes were refined, merged, or split.
5. Defining and Naming Themes: Each theme was defined clearly to capture its core meaning and contribution to the research questions.
6. Producing the Report: The finalized themes were used to structure the presentation of findings in Chapters 5, 6. Key extracts from participants were selected to illustrate each theme and highlight practical examples.

The codes were first developed and then refined iteratively as interview transcripts were reviewed, which allowed for inductive themes to emerge that captured the nuances of organizational behavior, perceived compliance obligations, escalation mechanisms, and socio-technical barriers in patching processes.

Coding was performed by the main researcher, who also conducted all interviews. While inter-rater reliability was not used as a quality measure, consistent with the nature of TA, regular peer debriefing sessions were held with supervisors at the participating company to discuss coding consistency, refine themes, and ensure that interpretations were justified with the underlying data.

To code the interview data, ATLAS.ti was used as the primary qualitative analysis tool. This application provides the tools for systematic labeling and tagging, grouping, and retrieval of coded segments across interviews. Codes were later clustered into categories and overarching themes, which align with the analytical structure presented in the results section.

Moreover, as Yin (2003) emphasizes, triangulation was used by comparing insights from different participant roles, such as system administrators, SOC analysts, risk managers, and consultants, and across the two regulatory contexts (DORA and NIS2). Convergence in their perspectives on patching constraints, policy interpretation, and documentation practices was used to improve the credibility of the

findings. The resulting themes and triangulation informed the structure of the findings presented in Chapters 5 and 6.

4.3. Validation of Results and Recommendations

To ensure the reliability and practical relevance of the interview findings, a two-step validation process was conducted. After coding and analyzing the semi-structured interview data, follow-up interviews were held with experienced consultants to validate and refine the thematic findings. These sessions served to confirm whether the identified challenges, patterns, and workarounds resonated with broader industry experience. Subsequently, the derived recommendations were further validated through a second round of short, targeted interviews with consultants to assess their feasibility and value in practice. This iterative validation process strengthened both the analytical interpretations and the practical grounding of the recommendations.

4.4. Ethics

The selection and recruitment of interview participants were handled by the primary researcher in their capacity. Participants at client organizations were contacted through consultants working within those client organizations, who helped identify relevant stakeholders based on their roles in patch management and regulatory compliance. The interviews focused on participants' professional experiences and responsibilities related to patch management and regulatory compliance. Prior to conducting interviews, ethical approval was obtained from the Human Research Ethics Committee at TU Delft. Each participant received a clear explanation of the study's aims and scope and provided written informed consent. This document outlined how the data would be used, any potential risks involved, and the intended research outcomes. Participants were also given the opportunity to review relevant sections of the final thesis that included their contributions or direct quotations. Additionally, they were informed that they could withdraw from the study at any time without consequence.

4.5. Mitigating the Shortcomings of Chosen Method

Despite the strengths of qualitative interviews in capturing rich and contextualized insights, several limitations inherent to this method must be acknowledged. One of the primary limitations is the constrained level of anonymity associated with interviews, particularly when they are conducted in person or in a professional setting (Saunders et al., 2015). Unlike anonymous surveys, interviews require participants to disclose personal experiences, opinions, or potentially sensitive information in a context where they may be identifiable. This limited anonymity may lead to social desirability bias, where participants adjust their responses to appear more favorable or align with perceived expectations, potentially affecting the authenticity and completeness of the data.

To mitigate this limitation, several measures were taken. First, all participants were provided with detailed information about the study and their rights, including guarantees of confidentiality and anonimity. No identifying information was included in transcripts or published outputs. Second, participants were reminded that their input would be treated anonymously and that there were no right or wrong answers. These steps aimed to ensure a setting of trust and reduce pressure to self-censor.

Another methodological limitation arises from the reliance on participants' memory (Dryden et al., 2024). Since many questions asked participants to reflect on past events or processes, there is a risk of recall bias. Participants may unintentionally omit key details, misremember timelines, or conflate different events, leading to inaccuracies in the data.

To address this, interviews were conducted with a diverse set of practitioners, including both operational staff and consultants, to allow for triangulation of perspectives. Where possible, information from different participants was compared to identify patterns and validate recurring themes. Additionally, interviews were semi-structured to allow clarification and probing for context, helping to reduce misunderstandings or surface more accurate recollections.

A central limitation of thematic analysis is its interpretative subjectivity (Braun & Clarke, 2022; Schweizer

et al., 2017). Since the identification and coding of themes depend heavily on the researcher's judgment, different analysts might draw varying conclusions from the same dataset. This can affect the consistency and replicability of the findings. To mitigate this, the analysis process in this study was guided by a transparent and systematic coding procedure, including iterative validation and discussions with supervisors at the consulting firm to ensure reliability and analytical rigor.

Additionally, thematic analysis lacks a standardized framework, which, while it provides flexibility, also makes cross-study comparison more difficult (Braun & Clarke, 2022). The absence of fixed analytical boundaries can hinder the cumulative building of knowledge across studies, as differences in thematic scope and depth may lead to inconsistent conclusions. This limitation was addressed by anchoring the themes in both empirical data and existing literature to improve coherence and comparability.

Finally, thematic analysis carries a risk of superficiality if themes are identified broadly without sufficient analytical depth (Braun et al., 2018; Trainor & Bundon, 2021). This was mitigated by conducting multiple coding cycles, focusing on the relationships between themes, and integrating quotes to preserve the richness of the data. The emphasis was on capturing the nuanced interactions between regulatory requirements and organizational patching practices, rather than merely labeling surface-level observations.

As with many cybersecurity research with large organizations, this study adopts a case study approach. While this allows for exploration of context-specific practices, organizational factors, and regulatory interactions, it also limits the generalizability of findings. Insights drawn from two large, security-mature organizations and interviews with consultants may not reflect the experiences of smaller firms or organizations operating in different regulatory or operational environments. However, the goal of this research is not to provide statistically generalizable claims, but rather to generate nuanced, practice-informed insights into the socio-technical and regulatory complexities of patch management. Moreover, Chapter 7 revisits this limitation by comparing the findings to existing literature and related case studies to further contextualize the relevance and transferability of the results.

4.6. Research Flow and Structure

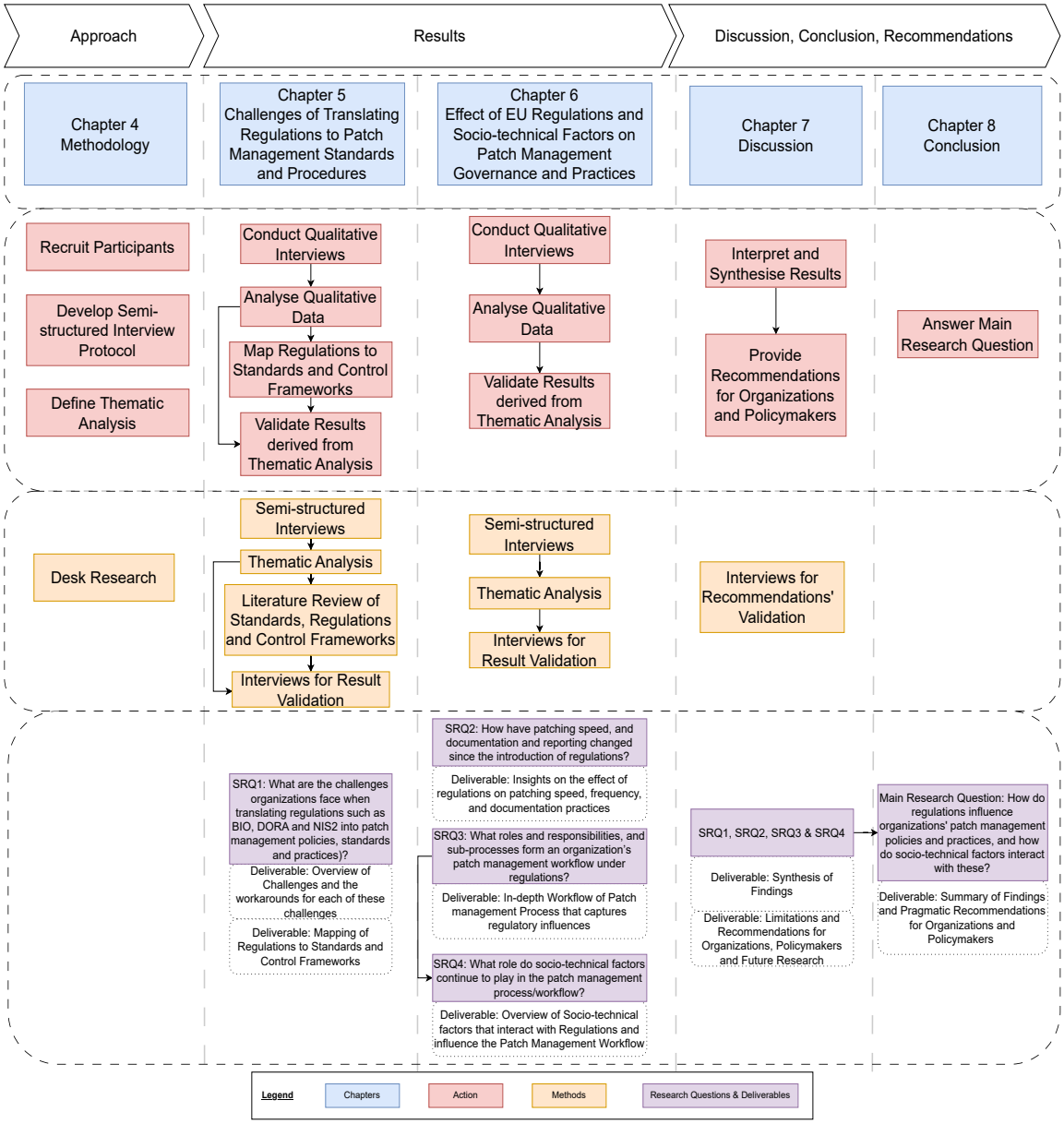

Figure 4: Flow Diagram illustrating the structure of the Methodology, Results, Discussion and Conclusion chapters. This includes the used research methods, the actions, the sub-research questions and deliverables.

The research followed a structured flow, as shown in Figure 4, that began with defining the methodology, where participants were recruited, a semi-structured interview protocol was developed, and thematic analysis was chosen as the data analysis method. The results were divided into two main chapters: first, identifying challenges organizations face in translating EU regulations into patch management policies and procedures, along with possible workarounds; second, exploring the effect of regulations and socio-technical factors on patch management governance and practices. Finally, the findings were synthesized in the discussion and conclusion chapters, providing recommendations for organizations and policymakers, as well as suggestions for future research to address unresolved issues in SSPM under regulatory pressures.

5

Challenges of Translating Regulations to Patch Management Policies and Procedures

Based on the interviews, several challenges were identified and coded, then grouped into overarching themes where appropriate. Each challenge described in this chapter represents one of these themes. For this reason, some challenges might have multiple dimensions to them. This was done in order to get an overview of challenges. These challenges arise not during the execution of patching activities themselves, but in the translation process and preparatory or background activities that need to take place aside from patching processes. Figure 5 gives an overview of the challenges in the translation process, the dimension of these challenges, and the workarounds that aim to alleviate or resolve these challenges. This subsection answers the first sub-research question:

SRQ1: ”What are the challenges organizations face when translating regulations such as BIO, DORA and NIS2 into patch management policies, standards and practices)?”

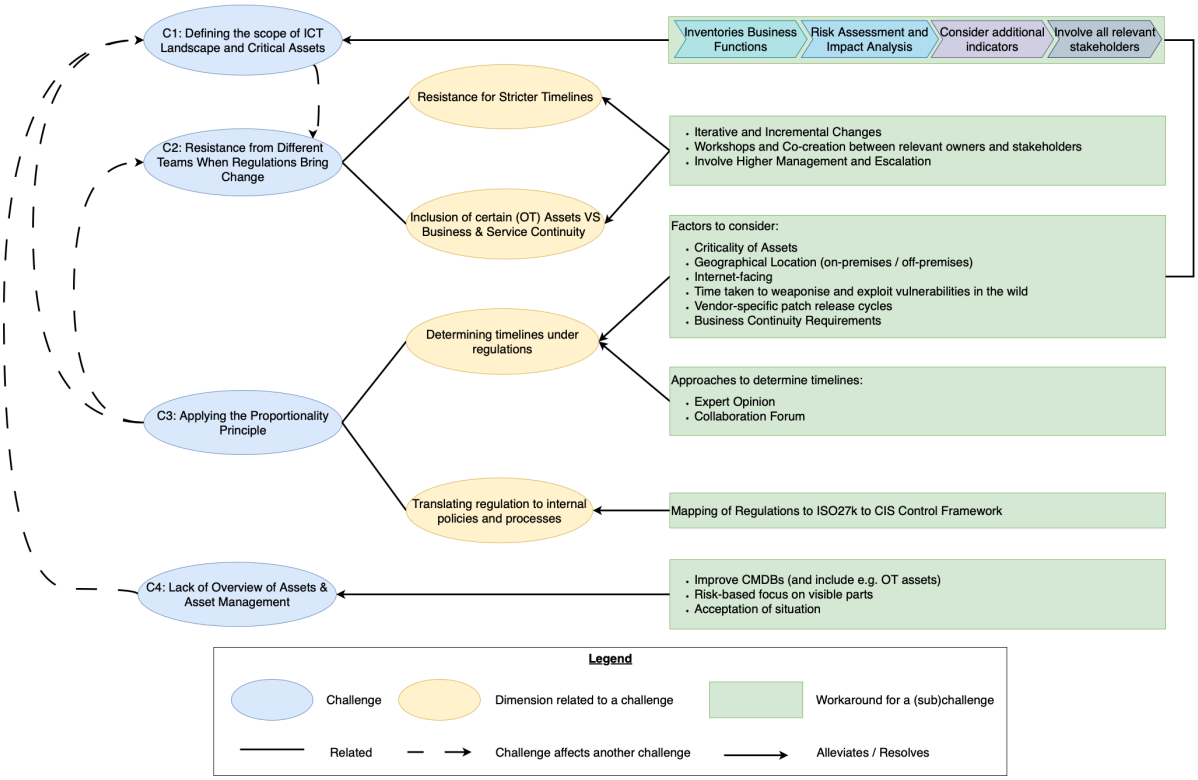

Figure 5: An overview of challenges related to translating regulations to internal policies and procedures, their dimensions, and the workarounds that aim to alleviate such challenges.

5.1. Challenge 1: Defining the Scope of the ICT Landscape and Critical Assets

Challenges

Participants noted that organizations struggle to define which assets fall under regulations like NIS2, and DORA, which use vague terms such as critical assets, essential services, and critical and important functions (CIFs). Organizations must interpret these terms and map them to their own assets, systems, and services This challenge of grows with the size and complexity of IT landscapes, which often combine legacy systems, cloud services, third-party applications, and decentralized infrastructure spread across multiple business units and regions. Internal debates about scope can further complicate decisions on which systems require frequent scanning, prioritization, patching, and intensive monitoring.

For example, under the introduction of DORA is the requirement to define and classify their ”Critical and Important Functions” (CIFs), as mentioned by P10. Although the regulation sets out that security patching and vulnerability management activities must be tailored to the classification of these functions, participants indicated that in practice it is not always straightforward to determine which systems, assets, or processes should be categorized as CIFs.

Under NIS2, the challenge varies by sector. In Case 2, the organization’s OT environments form hybrid ecosystems combining control systems and modern IT. Defining scope requires mapping interdependencies between IT and OT, which may involve identifying vulnerabilities that are physically isolated yet logically critical. In contrast, financial institutions typically map CIFs to business processes and related systems, such as payments and trading.

Workaround for scoping ICT landscape under regulations

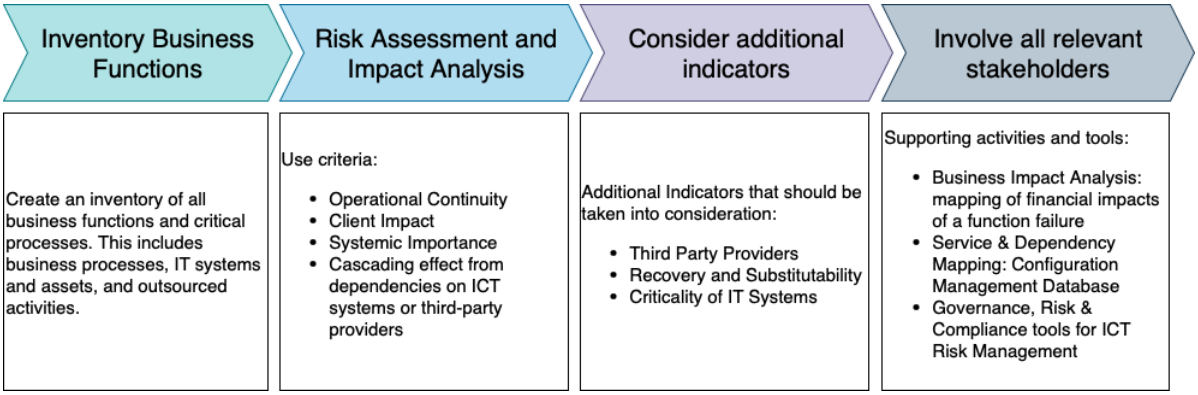

Figure 6: Workaround for determining the scope of the ICT landscape that falls under regulations

To address the challenge of defining scope, such as identifying CIFs under DORA, organizations follow a series of steps (Figure 6). According to P02, they begin by reviewing the definitions of CIFs, then conduct a Function Inventory, essentially listing all operational functions, including business processes, IT systems, and outsourced activities. This covers both core financial activities (e.g., lending, payment services) and support services (e.g., IT infrastructure, data management).

After, they should perform a risk and impact analysis. Luckily, DORA provides some criteria for this. These criteria are:

- Operational Continuity: Would a disruption prevent the organization from functioning?
- Client Impact: Would it significantly harm clients, investors, or market participants?
- Systemic Importance: Could a failure of this function destabilize the broader financial sector?
- They need to analyze the potential for cascading effects from dependencies on ICT systems or third-party providers.

After analyzing third-party risks, organizations must evaluate them by identifying functions heavily dependent on ICT providers, such as cloud services or critical software. They should assess the recovery time and substitutability of these functions—how quickly they can resume after a disruption and whether alternatives or redundancies exist. Functions that cannot be easily replaced are likely to qualify as critical or important under DORA, and, as P02 notes, may be subject to ”stricter timelines”.

The last step involves engaging the relevant stakeholders within the organization. This means involving relevant internal teams to gather their perspective into which functions are deemed critical or important. Some tools that help when involving key stakeholders are ”Business impact Analysis” (BIA). BIA maps the operational and financial impacts of a function failure. There is also some ”dependency and service mapping” done. ServiceNow and other CMDBs are example of service and dependency mapping. Lastly there is some ICT risk management or GRC software required to automate assessments.

5.2. Challenge 2: Resistance from Different Teams When Regulations Bring Change

Challenges

A second challenge that emerged from the interviews is that regulatory changes often encounter ”a lot of resistance” within organizations, especially when they require substantial updates to existing standards, policies, or operational routines.
This indicated that moving from an older version of a standard to a newer version, or integrating new regulatory requirements introduces many changes that must be embedded across various teams and processes. This can meet pushback from different stakeholders within an organization when the scale and feasibility of the new requirements are perceived as unrealistic or overly ambitious.

A clear example of friction arises between policy owners A clear example of resistance was observed for Case 1 between policy owners, who translate regulatory requirements into patch policies, and operational teams like the IT Department. Policy owners tried to set stricter timelines and requirements to align with regulations, while operational teams questioned whether such targets are achievable in complex IT environments. According to P01, this hesitation stems from also from uncertainty or “fear”about meeting new timelines given factors such as resource constraints, and the need to avoid business disruption.

Consequently, this led to negotiation and pushback from the IT department team which is responsible for actual patching, as said by P01. Stakeholders from the operational team brought up that they fear that stricter timelines for patching might not be as feasible. The same pushback was also noted around another related security task like penetration testing by P01. P01 mentions that ”it could be argued that it’s not a matter of fact that they know for sure, certain, that they cannot do this, but it’s more of a fear factor that they’re unsure whether these timelines are actually reachable.”

Another dimension of the challenge is the potential impact on business and service continuity. Interviewees noted that major changes to patching policies risk unintended disruptions if not carefully managed. Organizations must prepare their IT environments, align internal processes, and ensure security updates do not impair critical services for end users or customers.

In Case 2, resistance also did arise from teams managing Operational Technology (OT) assets, for which availability is the top priority and integrity and confidentiality are secondary. This contrasts with IT environments, which typically prioritize integrity and confidentiality alongside availability.

Because of this divergence in priorities, stakeholders managing OT resisted increasing patching frequency when driven by regulatory requirements. They view such interventions as potentially disruptive to critical operations, which raises concerns about downtime, instability of a system, or breaching vendor certification conditions. This can create friction between compliance and security on one side, and business continuity on the other.

Workaround for resistance to change driven by regulations

To address resistance from IT operations teams to stricter patching deadlines under regulations, organizations engage all stakeholders. According to P01, they hold workshops or working groups, where policy owners, process owners, operational IT teams, and other stakeholders can voice concerns, understand constraints, and negotiate feasible timelines. If consensus cannot be reached, P03 notes the issue is escalated to higher management, who either accept the risk of non-implementation or instruct teams to comply. P01 adds that timelines are often adjusted iteratively rather than abandoned.

To address this challenge, organizations primarily engage all stakeholders. P01 explained that organizations organize “workshops” or working groups, where “standard and process owners, operational IT teams, and other relevant stakeholders” come together. This allows participants to voice concerns, understand practical constraints, and negotiate feasible timelines. If an agreement cannot be reached, P03 noted that they “escalate the issue higher up in the organizations.” Once escalated, higher management “either accept the risk of not implementing the measure, or they tell the team that they do have to comply and move forward with it anyway.” P01 also described an “iterative way” of setting timelines: based on negotiations, new and stricter deadlines are adjusted iteratively rather than “being dropped” altogether. This approach leads to “a lot less pushback and people are more likely to buy into the changes because they feel heard and involved in setting the targets.”

5.3. Challenge 3: Applying the Proportionality Principle

Challenges

A key challenge identified by several respondents concerns the proportionality principle in NIS2 and DORA, and the difficulty of translating vague regulations into specific patch management policies.

These regulations are often high-level and generic, which creates ambiguity when applied to unique organizational environments. The proportionality principle acknowledges the diversity of organizations subject to these requirements, recognizing that a one-size-fits-all approach is impractical given variations in size, complexity, risk exposure, and resources.

As noted by P07, a critical subchallenge within this context is the setting of realistic timelines for compliance activities such as patching vulnerabilities. While their may be a mandate of certain deadlines, many organizations already struggle to meet these timelines due to factors such as ”resource constraints”. As a result, setting Service Level Agreements (SLAs) that are both compliant and achievable becomes a major pain point.

Interviewees also pointed to the challenge and difficulty organizations face in mapping regulations onto their internal standards and policies, as noted by P06. P06 mentions that ”regulations that they set are so generic that they don’t translate well to all the internal processes”. Since legislation typically do not specify detailed process flows, roles, or communication chains, organizations must develop their own internal standards and benchmarks to operationalize the requirements effectively.

Finally, the lack of clear guidance on classifying and prioritizing vulnerabilities complicates patch management. As P06 observed, definitions of what is considered a “high” or “critical” vulnerability are “debatable” and vary widely between organizations due to the proportionality principle, resulting in different prioritization methods and patching timelines. In the absence of a standardized guidance in legislation, organizations rely on internal risk assessments and risk appetite to address vulnerabilities. Participants also appear to reference the lack of guidelines for Operational Technology (OT) environments.

An important opportunity created by legislation like DORA and NIS2 is the introspection it forces on organizations regarding their risk profiles. Unlike the BIO framework, these regulations require organizations to define security needs and controls based on their own risk assessments. While this vagueness is challenging, it also encourages critical evaluation of patching strategies to meet actual needs. As P04 explained, it makes organizations ask, “‘Okay, what is actually my risk profile?’” P04 noted that this shift has been a valuable outcome of NIS2 and DORA, fostering deeper awareness of risk beyond patch management.

Workaround for applying proportionality principle

Related to determining timelines under the proportionality principle, main factors were derived to understand what organizations consider when deciding how quickly to apply software patches.

Patching timelines are strongly influenced by whether a system is considered critical. P01 and P02 referred to the “criticality of the application itself” or “the criticality of the operating system.” P02 also mentioned that the “geographical location of the system” is considered, distinguishing between on-premises and off-premises environments such as the cloud. Systems exposed to the internet carry higher risk and require faster patching, while, as P03 noted, if a system is “not connected to the internet directly and is in a segmented part of the network,” it may be ranked lower and assigned longer deadlines.

Organizations also assess how quickly vulnerabilities are exploited. P07 stated that “there is no strict benchmark,” but the time to exploitation is factored in, noting it typically takes “30 days to weaponize a critical vulnerability.” In the absence of a benchmark, P10 explained that timelines are largely set by “expert opinion” and peer comparisons. For example, in Case 1, the organization consults with others to align patching expectations, including through the Dutch “CISO Circle of Trust”, which is a collaborative initiative between major companies and the government to share threat intelligence, implement controls, and improve cyber resilience.

Finally, vendor patch release cycles are also considered. As P10 observed, “you could say it should be patched within seven days, but if [vendors] only deliver patches once every six months, that doesn’t make much sense.”

Another subchallenge that was identified was that the translation from regulations to internal standards does not always go smoothly because, to some extent, the proportionality principle leaves room for interpretation. Participants pointed out that while regulations and directives like NIS2 set high-level requirements, these do not translate directly into clear, actionable policies or controls. To cope with this challenge, organizations typically have to update their policies and standards, as mentioned by P10. They do so by interpreting and breaking down the regulations into objectives, and then specific controls that achieve those objectives.

Although it seems to depend on each organization on the approach, P04 mentions that a mapping is used for this. A mapping that connects the regulations directly to used frameworks like ”ISO/IEC 270002” and ”the CIS Control Framework” mentioned by P04, is provided in Appendix E. A dedicated framework is provided to help bridge the gap and link specific requirements from regulations to relevant standards such as ISO/IEC 27K and then to a controls framework such as the CIS Controls Framework. By doing so, organizations have an example of a structured way to interpret high-level legal requirements and turn them into specific and pragmatic measures that they can implement. This helps organizations define controls that are both compliant and practical for their patch management.

5.4. Challenge 4: Lack of Overview of Assets & Asset Management

Challenges

As P04 noted, a critical challenge, especially in operational technology (OT) environments, is maintaining a complete and accurate asset inventory. Unlike IT, OT often lacks clear guidelines or standardized “patching cadences,” and assets frequently go unregistered in systems such as the Configuration Management Database (CMDB). As P04 explained, “you don’t get a full view, and maintenance becomes very difficult.” This lack of visibility creates major security and compliance issues. Managing the environment requires all assets to be accounted for and monitored, typically via a CMDB or equivalent system. When OT assets are missing, organizations lose a holistic view, complicating maintenance and risk management.

The issue also connects to the first challenge (Figure 5) on defining the scope of IT landscapes and identifying which business functions fall under regulatory mandates. Without a comprehensive overview of both IT and OT assets, organizations struggle to define the scope of assets that falls under regulations. The complexity and uniqueness of OT environments further exacerbate these challenges, which requires a tailored approach to asset management.

Workaround for Lack of Overview of Assets

To address the lack of asset visibility, especially in OT environments, organizations often launch projects to improve their asset management. A common approach is developing or improving a Configuration Management Database (CMDB). As P04 described, these efforts are frequently initiated as “subprojects” within new vulnerability management programs, aiming to create a central source of asset information and provide a best-efforts overview of the environment. When organizations do not have the capability to improve their CMDB, they also often accept the situation of incomplete asset inventories.

6

Effect of EU Regulations and Socio-technical Factors on Patch Management Governance and Practices

This chapter explores if and how patching speed, documentation and reporting have changed since the introduction of the regulations. By studying the insights from the interviews, this section presents if the regulatory pressure has actually accelerated patching speed in practice and if so, and how it has influenced the way organizations document, and reporting on patch management. This chapter firstly answers the second sub-research question:

SRQ2: "How have patching speed, and documentation and reporting changed since the introduction of regulations?"

This chapter also shows how current workflows and processes are arranged in organizations, including the relevant stakeholders' roles, responsibilities, and processes. Together, this chapter provides a view of the practical impact of these regulations on day-to-day patch management in complex organizational environments. Furthermore, it shows how socio-technical barriers still play a role. This chapter answers the last two sub-research questions as well:

SRQ3: "What roles and responsibilities, and sub-processes form an organization's patch management workflow under regulations?"

&

SRQ4: "What role do socio-technical factors continue to play in the patch management process/workflow?"

Themes from the interview data relate to the complexity of patch management workflows and stakeholders' responsibilities under EU regulations. The data shows how patching processes have evolved to meet new regulatory requirements. To comply, organizations implement governance structures that divide roles and responsibilities among stakeholders, as reflected in the workflow diagram in Figure 7.

While Chapter 5 presents the challenges of adapting patch management policies to regulatory expectations, this chapter focuses on the barriers encountered in day-to-day execution under these regulations. In this study, challenges refer to the foundational and preparatory work, such as defining scope, mapping critical systems, that is needed before patching process can reflect the influences of regulatory

pressure. Barriers in this study, in contrast, involve the operational obstacles of remediation and patching itself, including coordinating across teams, managing legacy systems, and executing emergency patches under time constraints. Distinguishing these terms separates the structural conditions for implementing regulations from the practical realities of ongoing patch management.

6.1. Faster Patching under Non-prescriptive Regulations

Liability/Accountability mechanism

Interviews revealed that recent regulations affect not only the urgency and speed but also the frequency of patching activities. While most regulations do not prescribe strict deadlines, unlike the BIO or CISA's KEV BOD deadline for top-priority vulnerabilities, they require organizations to take timely measures to patch or mitigate vulnerabilities. Compliance is enforced primarily by holding management liable for meeting their own organization's patching deadlines.

P07 noted that under DORA, the management board is ”personally liable” if it fails to exercise ”due diligence” or demonstrate fulfillment of its responsibilities. This personal liability, combined with potential fines, increases accountability and drives management to prioritize compliance with patching policies and timelines. Interviewees repeatedly described this as a key incentive for strengthening vulnerability and patch management, particularly in larger organizations.

To meet regulatory obligations, many organizations translate high-level requirements into internal service-level agreements (SLAs) for risk-based patching timelines. These SLAs set maximum remediation timeframes by severity, which IT teams must meet. As P05 noted, “SLAs are embedded” in daily processes. By stating severity levels and deadlines upfront, organizations create accountability and ensure teams are aware of patching requirements.

If deadlines cannot be met, this triggers escalation or formal risk acceptance by senior management, as P03 described. P03 also mentions that significant delays or high-risk vulnerabilities are escalated through the ”incident management escalation”, involving crisis teams or committees with senior management. These scenarios typically unlock more resources than low-risk cases.

Another driver of patching speed is the link between vulnerability scanning and remediation. DORA, for example, requires weekly scanning for ICT assets supporting critical or important functions. P10 noted this requirement pushes others to increase scanning frequency from ”biweekly” or ”monthly” to a weekly basis, which is assumed to accelerate patching. A clear assumption here is that more frequent detection enables quicker remediation.

Notification and Reporting Obligations

Regulations can also indirectly accelerate patching through formal reporting obligations. When a critical vulnerability or significant incident is discovered, organizations are often legally required to notify regulators or the national CERT within a set timeframe. They must then provide a detailed follow-up, including a root cause analysis and proof of remediation. In some cases, this obligation extends to informing other organizations in the sector and, where appropriate, the public.

As P03 noted, reporting requirements add pressure on organizations to perform patching promptly and thoroughly to avoid reputational damage and demonstrate compliance. P07 explained that this expectation can also lead organizations to allocate more resources to vulnerability management, including hiring dedicated staff “to cover out-of-support business hours” to meet these obligations reliably.
This example shows how mandatory reporting and the risk of non-compliance can act as additional levers to push organizations to improve their patching processes and resilience. However, it must be noted that some aspects remain partly voluntary or sector-driven. For example, there is a mutual agreement among financial entities to not compete on cybersecurity topics. Therefore, when major vulnerabilities or incidents are discovered, they must share any relevant information with other financial entities.

6.2. Delays due to Documentation depend on Previous Regulatory Exposure

One frequently mentioned aspect of new regulations like DORA and NIS2 is their emphasis on documenting and reporting patch management activities. While regulations may not always specify how to prove compliance, reporting and documentation are seen as essential to "demonstrate how you're compliant." This has led to the implementation or expansion of structured risk and vulnerability reporting processes. P04 and P07 noted that organizations must now document not only deployed patches but also decisions to defer patches for certain systems or vulnerabilities that fall outside SLA compliance. P04 also highlighted the manual workload involved, such as "making all kinds of Excels."

The findings offer a nuanced view of whether increased documentation and reporting cause administrative burden or delay patching. A key factor is an organization's previous exposure to regulations. For highly regulated organizations in the financial sector like Case 1, proper documentation practices often predate DORA, so the regulations largely reinforce existing processes. In contrast, organizations newly subject to regulation, especially those soon to fall under NIS2, may be facing these requirements for the first time. For Case 2, building and maintaining reporting structures is a significant operational and administrative burden.

P04 and P06 indicate that many newly regulated large organizations are investing in automation to manage documentation and reporting more efficiently. Automation tools can generate logs, compliance reports, and dashboards with minimal manual effort. If implemented well, this reduces delays from administrative work and allows security and IT teams to focus on remediation. Still, as P06 noted, some manual effort will remain because "human oversight" is always needed for decision-making.

6.3. Workflow Narrative

Figure 7 depicts the practices of large, mature organizations with prior regulatory oversight and illustrates how socio-technical barriers can affect each process and decision point. The stakeholder group that benefits most from this complete workflow view is executive management, particularly the IT and Business management, because it links process details to regulatory outcomes. This visibility supports informed decisions on risk management and investments, effective resource allocation, and identification of process gaps. While other stakeholders in the diagram also gain clarity about the process, executives derive the greatest strategic value from seeing the full workflow.

The process begins when the SOC Analyst receives an initial vulnerability or patch notification. However, other methods of retrieving information about patches and vulnerabilities have been identified previously (Dissanayake, Jayatilaka, et al., 2022b; Jenkins et al., 2024). They conduct initial triaging by identifying affected assets through the CMDB or by consulting colleagues informally, and they retrieve the relevant technical details. If any assets are impacted, a main ticket is created and assigned to the appropriate solution group. The patching process is initiated with a ticket. If the identified vulnerability or patch are highly critical, an escalation is triggered where all relevant stakeholders are in a quicker and urgent manner. Here it is also important that analysts constantly maintain overview of the progress of the remediation process. This could also involve sending reminders about SLAs to stakeholders that need to remediate tickets or approve decisions. This in itself is a form of regulatory pressure.

From there, coordinators and maintenance groups take on a critical role in locating affected software, asset owners, and relevant teams. They reassign sub-tickets where necessary. Once the technical scope is clear, system administrators assess the applicability of the patch or vulnerability, perform risk assessments, and test patches in non-production environments. If testing is successful, patches are deployed by sysadmins to production systems, together with any required mitigation measures. The process includes verification steps and the collection of evidence to ensure completeness.

Before sysadmins deploy patches, system and asset owners, together with business process owners, evaluate risks within their domains and determine whether additional mitigation is required. They carry out their own testing where applicable and communicate decisions back to the system admin-

istrators. At the governance level, IT leadership, business management, and the Change Advisory Board assess risks from both infrastructure and business process perspectives. They set mitigation deadlines, approve or adjust proposed measures, and ensure that external reporting obligations are met, such as notifying regulators within one month of the initial notification and alerting other financial entities when a major vulnerability is discovered, as mentioned in Section 6.2.

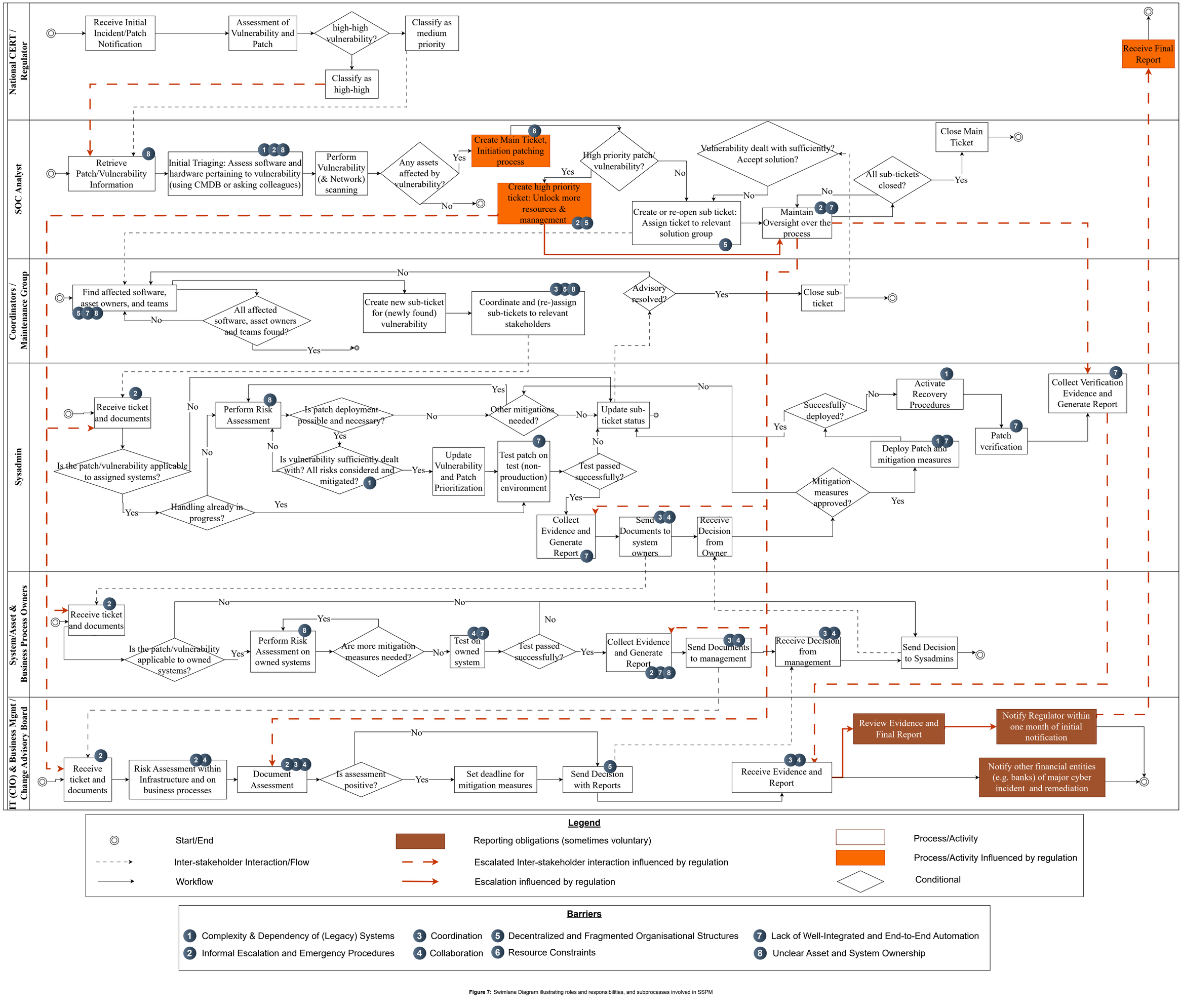

Figure 7: Swimlane Diagram illustrating roles and responsibilities, and subprocesses involved in SSPM

6.4. Socio-Technical Factors Act as Barriers and Enablers in Regulated Patching Workflows

During the interviews and the thematic analysis, several known socio-technical factors also emerged that seem to influence different aspects of the patch management workflow and process. The socio-technical challenges were coded, which were later grouped into themes of factors where it seemed reasonable. For this reason, a socio-technical factor might have multiple subfactors to them.

6.4.1. Complexity & Dependency of (Legacy) Systems

Barrier for Workflow

A major barrier to patch management is the technical and organizational complexity of legacy systems and their dependencies in modern, heterogeneous IT environments. Many organizations operate layered infrastructures combining outdated components, modern cloud systems, and interconnected services across multiple business units. These environments are challenging not only because of age and lack of vendor support, but also due to the dense dependencies between systems, applications, databases, and networks. This complexity increases the risk of unintended disruptions when patches are applied and complicates decisions on when and how to patch specific assets.

Participants noted that interdependencies can discourage patching due to fear of side effects. In industrial or operational technology (OT) settings, P03 explained, updating one component may cause failures in dependent systems requiring strict version compatibility.

Legacy systems further compound these issues. They often run on outdated middleware or platforms with no available patches, or where upgrades would disrupt dependent components. As P03 described, when no patch exists for a critical vulnerability, organizations may “isolate the system” instead. P10 added that some systems are “stuck in an old version of a platform,” forcing repeated decisions about whether to isolate the system, or accept the risk. In such cases, patching may be technically infeasible, and alternative mitigation measures add more coordination steps to the workflow.

Many legacy or non-internet-facing systems require manual patching, further straining resources. These systems often fall outside automated patch management tools and need direct coordination with asset owners or administrators. As P05 explained: “Since these systems are not internet-facing, they are not patched automatically through cloud services, so patches have to be applied manually.”

This barrier mainly affects three stages in Figure 7): assessment, testing, and deployment. In assessment, teams determine whether a patch exists and if it can be applied without disrupting dependent systems. In testing, they evaluate compatibility with upstream and downstream components, often requiring cross-functional coordination. In deployment, manual intervention, additional risk assessments, and phased rollouts are common, especially when systems are interconnected across departments or operate in safety-critical environments.

Relation to Regulation

Regulations influence this barrier in two ways. On one hand, they can act as enablers by promoting risk-based decision-making and incentivizing improvements in asset visibility and dependency mapping. For example, DORA’s classification of Critical and Important Functions (CIFs) and NIS2’s protection of essential services require organizations to understand system interdependencies and their impact on risk exposure. This has led some to adopt tools like ServiceNow to visualize interconnections and single points of failure, enabling more informed patching decisions.

On the other hand, regulations can also act as barriers when compliance timelines do not account for the complexity of patching legacy or tightly coupled systems. Requirements for timely remediation may conflict with technical constraints, forcing organizations to defer patches or seek risk acceptances—both of which require formal documentation and review.

6.4.2. Informal Escalation and Emergency Procedures

Barrier for Workflow

Emergency patching and escalation procedures are a crucial component of the patch management process to respond to critical vulnerabilities that require immediate remediation. However, they can be a barrier when in patch management since emergency patches frequently are informal and bypass the established cadence of deployment, which is the sequential testing and rollout across development and production environments. Instead, the process is sped up ”where we do the dev, test, and production patching together, instead of following the usual longer schedule”, as noted by PO4.
While expedited patching minimizes exposure to known threats, it increases the risk of instability or unforeseen side effects by shortening testing. One participant noted that in escalation scenarios, patches are deployed to development, test, and production environments within the same week, bypassing the usual observation period in testing. Although the workflow in Figure 7 assumes standardized sequencing of evaluation, testing, approval, and deployment, emergency situations often prompt informal, ad hoc deviations. In some organizations, the absence of structured emergency response mechanisms results in inconsistent handling of escalations, with decisions sometimes made via email and little formal documentation. P05 shows that even though the procedures for alerting and escalating critical vulnerabilities exist, they tend to lack structure and standardization in practice, e.g. ”emails” are used to send reminders of patch deadlines.

Relation to Regulation

From a regulatory standpoint, both DORA and NIS2 require organizations to have formal and documented processes for emergency patching and escalation protocols. In this sense, regulation acts as an enabler, pushing organizations to establish clearly defined escalation procedures and responsibilities. Formal emergency procedures are necessary to show compliance.

However, the description by participants suggests a gap between regulations and day-to-day operations. While regulations require formal procedures, many organizations continue to rely on informal, non-standardized communication channels and ad hoc decisions during emergencies. This misalignment presents a barrier in practice, as organizations may struggle to demonstrate that they have followed a formal process, even when the patch has been successfully applied.

6.4.3. Coordination

Barrier for Workflow

Coordination, both within teams and across departments,is a critical factor in effective patch management. Interviews revealed that fragmented practices, inconsistent processes, and siloed responsibilities can become barriers. When teams respond differently to the same vulnerability, e.g. P06 mentioned “if one team, for example, does their patching in one way and another team does it differently”, it “can cause a lot of disruption.” P06 added that this leads to “operational miscommunication” and ultimately a larger window of exposure.

This barrier affects multiple points in the workflow, particularly where decisions and documentation are exchanged between stakeholders. The difficulty arises when patching requires cross-functional coordination, such as between IT teams, application owners, and management (see Figure 7). These dependencies can delay action, especially when resolution depends on shared systems or platform-wide updates. P05 illustrated: “For instance, if we want to fix something but another team says, ‘This will be fixed by updating the entire Microsoft Office suite to the 2021 version,’ then we defer the vulnerability.”

Regulation has influenced coordination by pushing high-severity vulnerabilities to the top of the priority list. However, this often comes at the cost of low- and medium-severity vulnerabilities, which can accumulate in patching backlogs, especially when their remediation requires coordination across teams or departments. In this way, coordination overhead itself becomes a barrier to consistent patch deployment.

Relation to Regulation

To govern patching processes effectively, organizations assign clear roles and responsibilities, dividing duties among stakeholders. In this respect, regulation acts as an enabler by pushing organizations away from informal or fragmented practices toward centralized coordination, defined escalation paths, and unified patching policies.

Regulatory focus on business continuity, classification of critical assets, and patching SLAs has also driven more coordinated handling of high-risk vulnerabilities. Some organizations have introduced dedicated coordination or maintenance teams, particularly for systems deemed critical or in scope under regulations.

However, regulations can also act as barriers when they encourage reactive, high-priority patching at the expense of strategic coordination. Meeting strict timelines for critical vulnerabilities can divert attention and resources from building long-term coordination capacity. In highly distributed or decentralized organizations, these timelines may be unrealistic, as alignment across multiple stakeholders is required before a patch or mitigating measure can be implemented.

6.4.4. Collaboration

Barrier for Workflow

Effective patch management is a cross-functional effort involving IT departments, security teams, system owners, and business management. This collaborative dimension can itself become a workflow barrier. One example is DORA's requirement for organizations to map their Critical and Important Functions (CIFs). This forces security and IT teams to work with the business side to determine which systems support which functions and how they should be patched. As P03 explained, DORA encourages "organizations to think not just about everything as one big stack, but to also consider the systems and the business functions." This perspective requires active collaboration between stakeholders.

The tiered classification approach changes patching decisions from being based solely on vulnerability severity or system exposure to also factoring in business impact, including system availability and maintenance windows. The key question becomes not just "can we patch this?" but "can we patch this without disrupting a critical function or the financial system as a whole?"

In practice, this often results in a negotiation-driven workflow in which business owners, IT, and security collaborate to approve actions and allocate resources. This is especially relevant in decentralized organizations, where local system owners or departments manage their own assets and bear responsibility for patching decisions.

Relation to Regulation

Regulations attempt to enable collaboration by mandating patch management and vulnerability management policies that include definitions of responsibilities, roles and procedures. By bringing business management and security operations they push for collaboration, as alluded to by P03. This can act as an enabler for making better and more informed decisions on how and when to remediate vulnerabilities.

However, these same expectations can act as a barrier when organizations lack the right mechanisms to facilitate the required collaboration, such as the unclear roles and responsibilities or asset ownership (discussed in Section 6.4.8). In those cases, regulations inadvertently increase overhead, which can be time-consuming and add delays.

6.4.5. Decentralized and Fragmented Organizational Structures

Barrier for Workflow

A significant barrier is the organizational structure in which security and IT teams operate. In large, decentralized organizations, patching responsibilities are often split across teams managing different infrastructure components, application layers, or business domains. In one case organization, a central SOC and IT team existed, but asset ownership, business process ownership, and coordination roles were distributed across departments. This structural fragmentation complicates workflow coordination

and can delay or misalign patching efforts. It can also hinder the identification of affected software; as P05 explained, their team worked within an “availability management group” and depended on other sub-teams managing “sandboxes or servers.”

In such contexts, deploying a patch often requires coordination across teams with distinct objectives, processes, and resource constraints. For example, a security team may flag a critical vulnerability for immediate remediation, but implementation depends on another team responsible for scheduling patch windows or maintaining the underlying environment. This fragmentation creates friction, especially when teams operate semi-autonomously without clear communication, standardized workflows, or agreed priorities. Handovers can stall patching, particularly when systems span multiple business processes or when silos limit shared visibility into patch status.

Regulations such as DORA and NIS2 increasingly push for integration between security functions and business operations. Mandates for asset classification, weekly scans of critical systems, and vulnerability reporting foster a “closer relationship with the business.” As P10 noted, this shift not only brings “additional workload” but also embeds patching decisions more deeply into the organizational fabric.

Relation to Regulation

Regulations can also exacerbate organizational complexity. While they aim to improve risk visibility and protect critical functions, they impose stricter coordination requirements between security, IT, and business teams. In decentralized organizations, blurred accountability or unclear responsibilities for specific assets can delay patching.

6.4.6. Resource Constraints

Barrier for Workflow

Resource constraints are a persistent barrier to effective patch management under regulation, appearing as financial, time, and staffing limitations. These issues affect multiple stages of the workflow. Financial constraints can limit investments in automation tools, testing environments, or dedicated patch management teams, particularly in smaller or less mature organizations. Another cost that should be kept in mind is when disruptions cause systems to break or be incompatible. Without dedicated financial resources, scalable vulnerability management programs are harder to sustain, leading to patching delays.

Time limitations also create bottlenecks. Patches must meet service-level agreements (SLAs) that vary by severity, yet many organizations operate on fixed patch cycles (e.g., monthly). As P05 explained, “even critical patches often miss their SLA because they fall outside the monthly patch cycle.” These fixed windows limit flexibility for operational teams and the business, creating tension between regulatory urgency and internal scheduling.

Staffing shortages add another layer of difficulty. Patch classification, risk assessment, exception handling, and deployment often require skilled personnel from IT operations, security, and business teams. Even when tasks like vulnerability scanning are automated, follow-up decisions depend on human judgment. As P05 noted, “highly critical vulnerabilities are dealt with by people first, since those deserve the most immediate attention.” In such cases, staff availability or reliance on key personnel can delay remediation, especially when multiple vulnerabilities require immediate attention, further stretching already limited security teams.

Relation to Regulation

Regulation can act as an enabler through the proportionality principle, allowing organizations to meet requirements within their resource constraints while remaining compliant. It can also drive automation of workflow activities to reduce manual workload, though automation carries an initial cost.

However, regulations can also exacerbate resource constraints by raising compliance expectations without scaling the means to meet them. For example, mandatory weekly scanning of critical ICT

assets increases vulnerability detection, which expands the workload for scanning teams. If organizations are not resourced to address the resulting volume, barriers in patch assessment and deployment can worsen. As noted by P07, some have hired additional full-time employees to support incident management, including ”out-of-support business hours”. While certain organizations have reallocated resources or hired dedicated staff, these efforts remain uneven across sectors and organization sizes.

6.4.7. Lack of Well-Integrated and End-to-End Automation

Barrier for Workflow

Automation plays a critical role in streamlining patch management, especially in large, complex IT environments. As P05 noted, vulnerability and patch information is “integrated into ServiceNow” in one case organization, with most remediation activities—including classification, prioritization, and auditing—now largely automated. Tools like Tenable flag available patches for detected vulnerabilities, automatically assign severity levels, and route them to the relevant teams or asset owners, enabling a more prioritized and efficient response.

Despite these benefits, automation remains underutilized. Larger, highly regulated organizations tend to have more sophisticated automation, while more recently regulated organizations still rely heavily on manual processes for detection, prioritization, reporting, and auditing. A key limitation is the lack of end-to-end integration across tools and environments, particularly in hybrid infrastructures. P10 noted that while Tenable is used for most scanning, AWS platforms rely on separate tools and are “edge cases” outside some automation workflows. This results in parallel scanning tools, e.g., Tenable for most systems and separate scanners for AWS, which adds costs and requires manual work. For resource-constrained organizations, such gaps are especially problematic.

Even in settings where remediation is automated, some activities remain highly manual. As P05 explained, audit trails and documentation for patching decisions are still labor-intensive in newly regulated environments. Without centralized systems documentation and tracking systems, audit teams must manually compile evidence from different email threads, creating delays.

Relation to Regulation

For some organizations, regulations increase the documentation and reporting burden by requiring proof not only of what has been patched, but also of what remains unpatched and why. As P04 explained, “because the reporting that needs to be done indeed is intense. You not only need to report what you’ve patched, but also what you have not patched.” Sustaining this level of detail manually is difficult, particularly when reporting is monthly and in “increasing detail.” These inefficiencies drive a need for automation, with many organizations centralizing communication and evidence in systems like ServiceNow. On a best-efforts basis, emails, approvals, comments, and decisions are logged in one place, enabling quick, consistent evidence exports and reducing manual effort in the patching process. In this way, regulation pushes organizations to automate “on a best-effort basis.”

Organizations seeking to overcome manual process limitations often adopt centralized platforms like ServiceNow to consolidate communication and patch status updates. According to P04, regulatory pressure has already pushed some previously regulated sectors, such as banking, to adopt more automation and reduce manual work.

However, these improvements are not yet standard. Newly regulated organizations still rely heavily on spreadsheets and email-based escalation for coordination, audit preparation, and stakeholder communication. Many regulatory requirements—such as weekly vulnerability scans, adherence to internal patching deadlines, and detailed incident reporting—implicitly assume a certain level of maturity and automation infrastructure. For organizations without this foundation, such regulations can still function as a barrier.

6.4.8. Unclear System and Asset Ownership

Barrier for Workflow

A major barrier relates to establishing clear ownership of systems and assets within organizations. P04 notes: ”Who is the owner of the environment or who is the owner of a certain asset and can make the decision?” Ownership is required to make decisions regarding an organizations’ assets, such as approving or denying patch deployments. However, in practice, determining who holds ownership over an environment or specific asset can be ambiguous. This lack of clear ownership complicates decision-making processes, specially when an asset owner must decide whether to proceed with patching or file an exception.

Relation to Regulation

Regulations can act as both an enabler and a barrier in relation to asset ownership. On the enabling side, they often require organizations to assign formal ownership of systems and applications, creating accountability and a clear decision-making chain. For example, requirements to define control owners for security controls can compel organizations to designate responsible parties.

However, regulations can also exacerbate ownership challenges when compliance deadlines demand rapid action but ownership structures are unclear. If SLAs mandate patching within short timeframes, ambiguity over ownership can result in missed deadlines and non-compliance. Even when owners are defined, some may neglect their responsibilities, requiring coordinators or SOC analysts to send reminders and, in some cases, escalate the issue.

7

Discussion & Recommendations

7.1. Emergence of Workarounds as Adaptive Responses to Translation Challenges

The results in Chapter 5 pertaining to the first sub-research question reveal challenges in translating regulatory language into concrete patch management policies. One of the most fundamental challenges is applying and dealing with the principle of proportionality. While this core regulatory principle is intended to provide flexibility, it also introduces subjectivity and ambiguity. Organizations must align security controls with their risk profile, but without clear benchmarks, they may over- or under-invest in patching activities (Grima & Marano, 2021). This study shows that some organizations address this ambiguity by mapping regulatory requirements to control frameworks like ISO 27002 and CIS, which help standardize internal patching policies. A detailed mapping is included in Appendix E.

A separate challenge stemming from this ambiguity is scoping. Regulations like DORA and NIS2 introduce concepts such as Critical and Important Functions (CIFs), but do not exactly tell how to define them. Particularly for large and decentralized organizations, this leads to internal debates about which systems or services fall under scope. Other studies have already noted that classifying assets as critical under DORA is legally complex (Parchimowicz, 2024), and that overlap with regulations like NIS or MiCA further complicates this process (Avsuvarova, 2023). This study adds to the literature by showing that the classification process is not only legal or technical, but also political, requiring negotiation across departments. Large financial enterprises typically work around this by compiling an inventory of business functions and their supporting IT, OT, and outsourced services, and then evaluating these against DORA's four CIF criteria: operational continuity, impact, systemic importance, and cascading ICT dependency. Additional indicators such as third-party risks are also important, as shown by a recent breach of a third-party service Air France & KLM were using (Paganini, 2025). Lastly, organizations engage relevant stakeholders.

A challenge not explored in previous patch management literature, that also shows the need for managing competing incentives and negotiation, is resistance. Some IT or operational teams push back against regulatory timelines due to fear of infeasibility caused by the practical workload of patching, while some departments, especially in OT-heavy environments, may prioritize availability of their systems over patching and associated downtime.

The remaining challenge is the lack of a complete and up-to-date asset overview. Previous work notes this in general security terms (X. Li et al., 2016; ten Napel et al., 2024), but this study shows how asset management also impacts scoping of ICT Landscape. Without accurate CMDBs or asset management, organizations cannot determine which assets fall under regulatory obligations, which leads to difficulty when trying to become compliant to regulations.

Reflecting on these results, large organizations that already have had exposure to regulations, for example banks under DORA, had already developed practices and routines around vulnerability scanning,

classification of vulnerabilities, and escalation procedures. For these subgroup of organizations, new regulations like DORA then served more as minor adaptations to their existing practices or a reinforcement rather than a disruption. Newly regulated organizations, by contrast, showed more uncertainty around such topics. Other aspects such as asset management were also noted as challenges for newly regulated organizations. This shows an important dynamic. Compliance does not always emerge in response to regulations. In this sense, the presence socio-technical barriers (mentioned in Chapter 6) prior to regulations determines whether regulation becomes a catalyst for improvement or a source of friction in the beginning.

While the identified challenges are significant for newly regulated organizations, this study still shows adaptive capacity. Large financial entities had developed workarounds to cope with the challenges introduced by the DORA regulation, as seen in Chapter 5. These workarounds are not ideal, but they are instructive. They show that organizations actively try to close the gap between policy and practice.

Importantly, the use of workarounds is not necessarily a sign of immaturity. In some cases, they reflect pragmatic decisions to manage complexity in the presence of ambiguous regulations and the challenges of asset management. However, for newly regulated large organizations, they also point to areas where effective translation of regulations is limited by systemic issues such as lack of early engagement and involvement of relevant stakeholders, or competing incentives of e.g. including OT systems in patching cycles.

7.2. Differential Impact on Patching Speed and Documentation

The results in Sections 6.1 and 6.2 pertaining to the second sub-research question reveal how regulations affect patching speed, and documentation and reporting. Where ten Napel et al. (2024) focus on the BIO regulation's one-week patching deadline, this study examines the effects of non-prescriptive regulations like DORA and NIS2. Despite lacking fixed remediation timelines, these regulations can still accelerate patching by increasing board-level liability for non-compliance, mandating weekly scans, and obligating the reporting of significant vulnerabilities or patching practices. These approaches increase the urgency to patch and enable faster escalation of unpatched critical vulnerabilities, particularly when an organization's SLAs are defined and enforced internally.

A key differentiator compared to BIO is the regulatory obligation under DORA to scan ICT assets weekly, especially those tied to critical functions. This ensures earlier detection and potential remediation of vulnerabilities. Moreover, requirements on organizations having to report "significant" vulnerabilities and incidents to regulators, absent in the study by ten Napel et al. (2024), drive organizations to improve response processes and sometimes assign dedicated roles to incident response.

However, such regulatory pressure does not guarantee improved outcomes in all settings. Its effectiveness depends heavily on how much an organization has been exposed to regulations previously. Large organizations that have been exposed to regulations use them to reinforce existing processes and workflows, which can increase; Newly regulated organizations might struggle without sufficient automation or structured processes.

On documentation and reporting, findings challenge the view that such obligations inherently delay patching (ten Napel et al., 2024). Instead, this study finds the impact to be context-dependent. For regulated or mature organizations, reporting strengthens accountability. For large, but newly regulated or less mature organizations, particularly with complex OT environments, it introduces friction that demands some technical and procedural investment.

This variation may be explained by the proportionality principle. Since regulations allow organizations to adapt controls based on size, risk, and capacity, the burden of documentation and reporting differs significantly. Proportionality permits flexibility in how documentation is structured, but once policies are formalized, compliance is strictly expected.

Previous research viewed patching as primarily the responsibility of system administrators (Jenkins

et al., 2024). ten Napel et al. (2024) added that regulations reduce sysadmin discretion. This study nuances that position. It finds that while DORA and NIS2 introduce regulatory pressure, the proportionality principle enables shared discretion across multiple stakeholders, SOC analysts, coordinating teams, asset owners etc. Organizations retain freedom in defining policies, but once set, compliance is required. Thus, discretion is allowed in design, but constrained in implementation.

Reflecting on the results, there seems to be an uneven impact of regulation on patching speed and documentation. Participants noted that regulations tend to accelerate patching for high-profile vulnerabilities, but less so for lower-severity issues. Documentation requirements, on the other hand, have added overhead across the board for newly regulated organizations that still rely on manual processes. For many newly regulated large organizations, this has initiated a shift toward automation, not only for patching itself, but also for reporting and tracking compliance for example.

Yet, automation is not uniformly accessible across organizations. Larger and more mature entities often have access to automated dashboards and integrated workflows that support patching, documentation, and reporting. In contrast, smaller organizations, particularly those that were not previously regulated or considered critical, may still rely on manual processes, such as tracking patches in spreadsheets. While previously regulated organizations typically have the resources to invest in automation tooling and move forward from manual processes, newly regulated ones often lack the capacity or budget to do so. This disparity not only limits their ability to comply efficiently but also exacerbates inequalities in compliance. This shows how the effectiveness of regulation is closely tied to internal capabilities of an organization.

7.3. Persistence of Socio-technical barriers in Patch Management Workflow

This research reconstructs the patch management workflow that mature, previously regulated organizations follow under regulatory pressure, drawing on interviews and insights from ten Napel et al. (2024) in Sections 6.3 and 6.4. The resulting workflow in Figure 7 goes beyond the more linear, technically focused patch management workflow proposed by Gentile and Serio (2019), which concentrates primarily on a limited set of technical patching processes and stakeholders. In contrast, this study incorporates several interdependent sub-processes and emphasizes the roles of many more stakeholders, including SOC analysts, system administrators, asset owners, business process owners, and both business and IT management. It further situates these roles in the context of socio-technical barriers, which shows how regulations not only influence what and how fast something gets patched, but also how the process is structured, coordinated, and governed.

What is notable based on the constructed workflow is that it demonstrates a notable shift in power and influence within the regulated patch management workflow, which is visualized in Figure 8. Traditionally, operational stakeholders such as SOC analysts and sysadmins have had significant autonomy in handling vulnerabilities, with decision-making power concentrated at the technical execution level. However, Figure 8 shows that regulatory compliance, governance requirements, and cross-functional dependencies have elevated the strategic role of IT leadership and business management into the ”Manage Closely” quadrant. This shift is further evidenced by the movement of sysadmins and coordinators/maintenance groups toward the bottom side of the quadrant, which indicates a remaining relatively high power in patch management process, but with relatively less decision-making power compared to leadership. The Change Advisory Board, although still in the ”Keep Satisfied” quadrant, retains high power but operates with lower day-to-day involvement.

Decision-making authority is migrating upward toward governance stakeholders, who now directly influence timelines, escalation procedures, and the acceptance or rejection of risk. This aligns with the regulatory trend in regulations like DORA and NIS2, which make patch management not just a technical maintenance task but a board-level liability item. The implication is that the patch management process has become a strategic risk management function rather than solely an IT operational process. While this may improve accountability and ensure business-aligned prioritization, it also introduces the possibility that operational agility could be constrained by additional approval layers, especially in time-

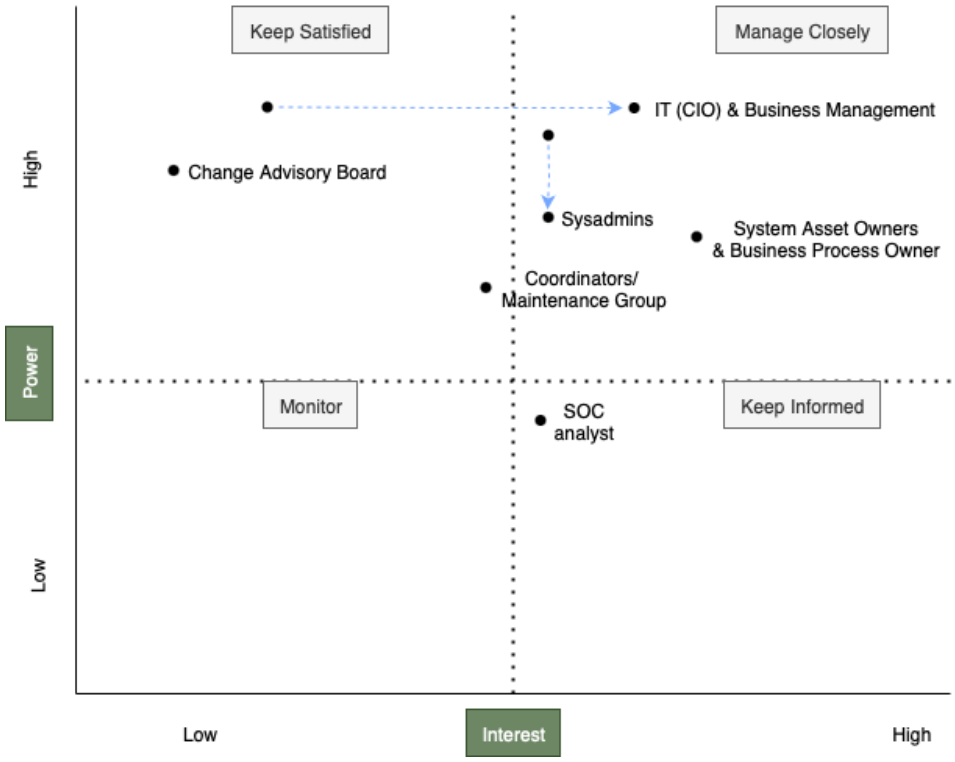

Figure 8: Power Interest Diagram illustrating the relative power and interest of the stakeholders mentioned in Figure 7.

critical scenarios. For this, informal escalation procedures will always exist.

Regulations such as the NIS2 Directive and the DORA Regulation shape this workflow by imposing requirements for scanning frequency, remediation timelines, documentation, and escalation procedures. These obligations influence every stage of the process, from detection to closure, embedding compliance checkpoints into operational workflows. For example, DORA mandates more frequent vulnerability scanning, which increases the cadence and resourcing needs for the discovery phase. Vulnerabilities are typically detected through automated scanners (e.g., Tenable, Rapid7), third-party threat intelligence, or public vulnerability databases, though other sources have also been identified previously (Dissanayake, Jayatilaka, et al., 2022b; Jenkins et al., 2024).

Once vulnerabilities are detected, the classification and risk assessment phase begins. This stage involves triaging vulnerabilities based on severity, exploitability, and potential business impact (ten Napel et al., 2024). Input is required from both technical experts (e.g., system administrators) and asset owners, who understand the operational criticality of the affected systems. Regulatory expectations reinforce the need for formal classification mechanisms and documented remediation decisions. In some cases, these frameworks also require demonstrating that risk-based prioritization aligns with documented internal service-level agreements (SLAs).

Following classification, assignment and coordination activities occur. Security analysts notify the relevant asset or system owners, outlining the vulnerability, its severity, and the remediation deadline. This step depends heavily on clear asset ownership, which remains a socio-technical challenge when organizational structures are fragmented or system responsibilities are unclear. Regulations indirectly strengthen this step by requiring traceable accountability, particularly in audits and incident reports.

Patch planning and testing then follow. Patches are often tested in sandbox or pre-production environments, sometimes in collaboration with business process owners to schedule maintenance windows for mission-critical systems. Here, socio-technical factors such as cross-team coordination and resource availability become significant bottlenecks (Dissanayake, Jayatilaka, et al., 2022b; ten Napel et al.,

2024). Regulations can add complexity by requiring dedicated testing environments, which may be costly or impractical for resource-constrained organizations.

Deployment and remediation form the core of the workflow. System administrators apply the patch, or if patching is not possible, implement alternative mitigation measures. When remediation is delayed, formal risk acceptance must be documented and approved by management. Regulatory frameworks reduce the discretion traditionally held by system administrators, requiring that deviations be fully traceable and justified.

After deployment, verification and documentation are critical. Remediation is confirmed via automated scanning tools or manual checks, with the results logged in ticketing systems such as ServiceNow. Compliance and audit teams collect this evidence for regulatory submissions. Past vulnerabilities such as Log4J have demonstrated how crucial this stage is for both internal assurance and external accountability (Dissanayake, Jayatilaka, et al., 2022b).

The workflow concludes with reporting and escalation. If SLAs are missed or remediation is delayed, the matter is escalated to senior management or incident response teams. In some cases, legal obligations require notifying regulators or national CERTs within 24 to 72 hours, as well as informing other (financial) entities. Management typically own this step to ensure that the organization meets all notification timelines. This step, largely absent from ten Napel et al. (2024), is essential under regulations.

Alongside these structured steps, socio-technical factors continue to exert significant influence, often amplified by regulatory demands. Legacy systems, with their complexity, outdated platforms, and interdependencies, remain a major barrier to timely patching (Gerace & Mouton, 2004). The inclusion of OT assets in the regulatory scope adds further complexity, particularly in risk assessments and testing. Despite formal escalation procedures mandated by regulations, many organizations still rely on informal escalation in emergencies, deploying untested patches outside standard cycles (Dissanayake, Jayatilaka, et al., 2022b). Coordination remains hindered by fragmented communication channels and manual follow-ups (ten Napel et al., 2024; Tiefenau et al., 2020). Collaboration is also intensified by regulations like DORA, which require joint prioritization between IT and business units through classifications such as Critical and Important Functions (CIFs).

Organizational structure also plays a role, with partially centralized security functions often delegating execution to functional teams (Jenkins et al., 2024; Kraemer & Carayon, 2007). Human and financial resource constraints persist across multiple stages, from information retrieval (De Smale et al., 2023) to patch testing (ten Napel et al., 2024), and the lack of integrated, end-to-end automation forces heavy reliance on manual work.

To reflect on these results, the persistence of socio-technical barriers (e.g. legacy systems, unclear ownership, decentralized organization, and limited automation) indicates that regulatory compliance alone does not guarantee efficiency of the workflow. In fact, regulations can amplify existing challenges by imposing higher scanning frequencies, tighter timelines, and more rigorous documentation demands. For newly regulated organizations, the ability to manage these socio-technical barriers will determine whether compliance to regulations translates into actual resilience, or remains a box-ticking exercise.

7.4. Recommendations for Organizations

Based on the discussion, some lessons from previously regulated large organizations can be learned for large organizations that are newly regulated.

1. **Adopt Established Practices under Regulations to Ease Translation Process and Shorten the Learning Curve**

    - Newly regulated large organizations can benefit from the established structures, processes, and workarounds already embedded in previously regulated sectors. As Chapter 5 shows, DORA-regulated large organizations tend to exhibit higher maturity in patch management

because regulatory oversight has long shaped their practices. For instance, the practice of mapping regulatory requirements onto established security standards and control frameworks (Appendix E) emerged as a concrete way to reduce the ambiguity of proportionality, turning abstract obligations into actionable, measurable controls.

A clear example is the classification of critical systems. Whereas NIS2 does not define explicit criteria for determining which systems fall under its scope, DORA requires organizations to assess business functions against four defined criteria, supported by business impact assessments and stakeholder input. NIS2-regulated entities could adopt this structured process to avoid inconsistent or ad hoc scoping decisions.

Adopting such practices early, before new regulations like NIS2 are transposed into national law, they can bypass the “learning curve” delays experienced in earlier translation stages. Furthermore, they can also use the proposed workflow in Figure 7 to assess their own processes, capabilities, functions (staff), and tools and find gaps. These gaps can inform improvements to their own processes. Though, these practices don’t emerge overnight but rather evolve through years of having a ”security culture” and compliance experience. An important aspect of effective patch management is the continuous cultivation of a cybersecurity-conscious culture (European Union Agency for Cybersecurity, 2021). In other words, by proactively embedding proven practices rather than waiting to react under compliance pressure, newly regulated organizations can reduce both the friction of implementation and initial compliance gaps.

2. **Co-designing Softer and Different Patch Policies to Address Resistance**

   - The challenge of resistance was most pronounced in large organizations, particularly when centrally defined patch deadlines were perceived as unrealistic or when OT assets were required to follow the same patching processes as IT assets. In several cases, this resistance was rooted in fear, often because similar deadlines had never been achieved before. As Malhotra et al. (2021) note, teams may resist even beneficial changes if they conflict with what is considered legitimate or acceptable within the organization.

     Reducing this resistance requires early involvement of stakeholders in the policy-setting process. Structured workshops where security, IT operations, and business management jointly map critical assets, define risk appetite, and negotiate remediation timelines have proven effective. This is similar to findings on co-design and stakeholder engagement from other domains (Blackwell et al., 2017; Eyles et al., 2016; Gooch et al., 2021; Harrington et al., 2018). ENISA also recommends fostering employee buy-in by clearly communicating patching objectives, openly supporting departmental input, and embedding these commitments in accessible, specific policies (European Union Agency for Cybersecurity, 2021).

     However, adopting co-design provides no guarantee that equal partnerships will be enabled between the different stakeholders (Farr, 2018) and “listening sessions” that ignore stakeholder concerns can erode trust. Co-designing must focus on genuinely incorporating feedback, sometimes by softening deadlines or differentiating policies to reflect the reality of patching. If resistance stems from IT/OT convergence, where OT assets are expected to follow the same processes and deadlines as IT assets, then adopting separate patch policies may be beneficial. Although this could introduce more overhead to manage compliance, eliminating resistance is ultimately more important. ten Napel et al. (2024) already mention the need to develop patch deadlines and practices that are not liabilities and have multiple policies. Such adjustments not only improve feasibility to comply with regulations, but also help overcome resistance stemming from fear. In this way, patching SLAs become both risk-aligned and practically achievable.

3. **From Superficial Compliance to Meaningful and Realistic Remediation**

   - As seen in Chapter 6, socio-technical barriers in patch management will persist due to the inherent complexity of IT environments. What organizations need is a more risk-based ap-

proach that focus resources on the most critical known assets and vulnerabilities, and preserving capacity to respond quickly, rather than chasing an unattainable ideal of perfect coverage or automation across all systems. This ensures that efforts are directed where they yield the greatest reduction in risk.

For example, trying to have complete automation is unrealistic, as many steps in the workflow in Figure 7 require a human in the loop to make decisions and ”edge cases” might still require manual scanning, for example. Another persistent barrier in Chapter 6 is limited visibility of assets. Pursuing a perfectly accurate CMDBs is often unattainable, especially when OT assets are involved and “unknown unknowns” exist. Perhaps, instead of this, organizations can focus on critical third-party risks or have more reserved capacity to respond to critical vulnerabilities and patches for known systems when they emerge.

Furthermore, instead of relying solely on reminders to patch (as in Chapter 6), large critical organizations could designate security champions (as mentioned by Aalvik et al. (2023) and Jaatun and Soares Cruzes (2021)) and ”change agents” who can steer teams away from opting for shortcut mitigation measures, such as temporary workarounds or partial fixes, that may formally satisfy compliance to regulations which require ”patch or mitigate”, but fail to deliver lasting or effective remediation. This idea of security champion also links to the idea of softer but achievable policies from the previous recommendation, which, if well-designed, can encourage more meaningful patching rather than superficial compliance.

7.5. Recommendation for Policymakers & Regulators

1. **Use of Soft Governance Aside from Binding Legislation**

- The results reveal that ambiguity in regulations and the lack of practical government guidance leave organizations uncertain about how to effectively comply. Beyond binding legislation, soft governance can be used which can help bridge this gap. For this, benchmarking and sector-specific cooperation forums are considered important to e.g. European Union’s Open Method of Coordination (OMC).

  Benchmarking, defined as establishing standards “by which something can be measured or judged” (Seng et al., 2009), enables organisations to compare their patch management performance with peers and identify best practices. Policymakers could support the systematic collection and publication of anonymised data on key metrics disaggregated by sector and organization size. Unlike static evaluations, benchmarking is normative in nature (Breakspear, 2012; Silva-Castañeda, 2016), and guides organisations toward improvement by highlighting achievable sector norms (Maheshwari & Janssen, 2014; Schellong, 2010). This evidence base would allow regulators to refine what “timely” remediation means in practice, replacing one-size-fits-all deadlines with realistic, data-driven targets, while giving organizations a defensible reference point for investment decisions.

  However, many organizations, especially SMEs or newly regulated ones, might not have the infrastructure or resources to collect and provide patch management data in a way that’s useful for others. Benchmarking should be accessible for different type of organizations. Therefore, policymakers could focus on providing such organizations the means to accurately collect and provide data on patching.

  In addition to benchmarking, another form of soft governance is facilitating sector-specific cooperation forums, such as the CISO Circle of Trust in the Netherlands, where security leads from peer organisations and regulators can exchange patching practices, and reference timelines under regulation. However, if sharing patch management practices through cooperation forums is perceived to create competitive disadvantages, organizations may be reluctant to participate. Therefore, the focus should be on fostering a shared commitment to treat security, and specifically patch management in particular, as a non-competitive domain, where all organizations agree that safeguarding the ecosystem outweighs individual

advantage.

7.6. Study Limitations & Recommendations for Future Research

7.6.1. Generalizability of Findings

Like much research in the field of organizational cybersecurity, this study is inherently case-driven. This shows the practical difficulty of getting access to IT practitioners within organizations, especially in sensitive areas such as security patch management. As a result, the research draws on a limited number of interviews from two large case study organizations, supplemented with perspectives from consultants. While having two case studies under different regulations and sectors allows for meaningful depth, it inevitably raises questions about the generalizability of the findings to other organizations' contexts.

The two organizations studied operate at a scale at which they can afford capabilities such as dedicated Security Operations Centers (SOCs). In contrast, smaller organizations, especially those without a designated IT function, may face entirely different challenges and barriers. This limits the ability to extrapolate these findings to small organizations or organizations that are constrained in resources. However, many of the challenges identified are not unique to the participating organizations.

This research is particularly relevant to newly regulated large organizations with a decentralized structure, where responsibility for patch management is distributed between a central IT function and various departmental stakeholders. The findings provide practical insights into how regulatory pressures and socio-technical factors manifest in such environments, and they can support reflection and improvement in organizations with comparable governance models. Nonetheless, no conclusions can be drawn about generalizability based on the absolute size of the IT environment or the number of end-users involved. These factors were outside the scope of this study.

While consultants provided a broader view of patching practices across different sectors and organizations, this perspective was still limited in terms of first-hand experiences from certain sectors, such as public administration. Future research would benefit from extending the dataset to include more diverse organizational types, including small and medium-sized enterprises (SMEs) and public sector organizations. A comparative multi-case study approach involving organizations of different sizes and across both public and private sectors would allow for more systematic exploration of variations in different contexts.

Finally, while this research provides actionable understanding for practitioners, it also reinforces that there is no singular or optimal solution to patching under regulatory pressure. Challenges and barriers will persist, but improved awareness of the socio-technical dimensions of patch management can help reduce the impact of those challenges. The findings may support IT managers and decision-makers in evaluating and refining their own patching processes, even though prescriptive guidance will always be limited by the inherently context-dependent nature of this domain.

7.6.2. Methodological Limitation

This study employed a qualitative research design to explore how organizations approach security patch management under regulatory pressure. While this approach proved valuable in discovering the socio-technical and organizational dynamics of patching, it also presents limitations, particularly in relation to the absence of quantitative data. Unlike studies such as ten Napel et al. (2024), which integrate measurable indicators of patching activity, this research does not include empirical data on patching speed, delays, or compliance rates. Although the selected case study organizations were large and presumed to have mature patch management policies, thereby increasing the likelihood of accessible quantitative data, such data were ultimately not available for inclusion. This shows the challenge of gaining access to sensitive data.

As a result, this study offers limited insight into the measurable aspects of patching performance under regulations. It cannot, for instance, quantitatively determine whether and to which magnitude patching speed has improved under DORA or NIS2 compared to BIO, nor can it identify statistically significant

causes of delay. To address this gap, future research should consider investigating organizations that actively collect and use patching metrics in their decision-making. This would enable a mixed-methods design that combine the depth of qualitative insights with the generalizability and rigor of quantitative data.

In addition, a mixed-methods approach could help mitigate common limitations of qualitative interviews, such as participant bias, social desirability in answers, or influence from hierarchical pressures within the organization. There is a reliance on self-reported data obtained through semi-structured interviews in this research. While interviews provide valuable knowledge about practitioners' perspectives and lived experiences, they are also susceptible to social desirability bias and selective recall. Participants may unintentionally portray their organization's practices as more compliant, structured, or mature than they are in practice, especially when discussing regulatory compliance or security procedures. Additionally, certain operational shortcomings or informal workarounds may be underreported or framed as exceptions rather than recurring patterns. This poses a risk to the validity of the findings, as the perceived patch management process may differ from actual day-to-day practices.

Future research could benefit from triangulating interview data with direct observations, internal documentation, or system-level patching metrics to mitigate this limitation and capture a more accurate picture of organizational behavior. Quantitative measures of actual patching activity could validate or challenge self-reported practices and perceptions. Ideally, such an approach could take the form of a longitudinal case study which allows for a more nuanced understanding of patching performance and regulatory pressure over time. Integrating such data with interview data would yield a more comprehensive view of how regulatory pressure by NIS2 and DORA influences patch management in practice.

7.6.3. The Evolving Nature of Regulations

An additional limitation relates to the evolving status of regulations, specifically regarding the NIS2 directive. At the time of this study, NIS2 had not yet been formally transposed into Dutch national law through the Cyberbeveiligingswet (CBW). As a result, the practical enforcement mechanisms and precise compliance expectations remain undefined. Consequently, it is not yet possible to empirically assess how NIS2 will affect patching speed or timeliness in practice. However, many organizations are already anticipating these changes and beginning to align their internal practices with the expected regulatory requirements. While organizations' anticipation of requirements provide insight into the perceived regulatory influence, they do not reflect actual enforcement. Therefore, findings concerning the influence of NIS2 should be interpreted as forward-looking and provisional which are influenced by organizational expectations rather than legal obligation. Further research will be needed once the CBW, or alternative national transpositions of the NIS2 Directive in other EU Member States, is in force and organizations must demonstrate compliance to those.

In parallel, developments are also underway regarding the Dutch BIO2 mandate, which is a forthcoming revision of the existing BIO regulation. Although the updated BIO2 is not expected to introduce stricter deadlines for patching, it may improve procedural expectations or increase scrutiny on patching behavior and practices. For example, BIO2 potentially can require improvement of analyses on threats and threat intelligence, which is relevant for information retrieval phase. It remains to be seen whether the introduction of BIO2 will lead to accelerated patching timelines in practice, or whether it will primarily serve to reinforce existing security standards. As such, both NIS2 and BIO2 show changing regulations that this study can only partially anticipate, and which warrant further research once those regulations are implemented.

7.7. Theoretical and Societal Relevance

This study advances current knowledge on software security patch management by (i) identifying concrete challenges that arise when organizations translate non-prescriptive regulations, and documenting the workarounds practitioners and organizations use. One key example is the mapping provided in Appendix E. (ii) It reconstructs a regulated patch-management workflow that is more extensive than linear, technical models of e.g. Gentile & Serio's 2019: it has a detailed focus on each sub-phase of patch management process; it embeds governance and decision-making, escalation, and documentation and

reporting duties, and a visible shift of decision power to IT and business management under regulatory pressure. (iii) It extends previous literature on socio-technical factors (e.g. Dissanayake, Jayatilaka, et al. (2022b), Jenkins et al. (2024), and ten Napel et al. (2024)) by showing how regulation interacts with known barriers, sometimes amplifying them, or sometimes pressuring organizations to bring improvements (e.g., automation). In short, regulation functions as both catalyst and enabler within the socio-technical system.

For the societal relevance, the workflow provides IT and Business management of organizations with an end-to-end view they can use to compare it to their own context to make decisions for investments, allocate responsibilities, and spot process gaps, especially in organizations that have not yet formalized the processes described. Newly regulated organizations can shorten the learning curve by adopting observed workarounds. Furthermore, it shows how organizations should consider involving stakeholders effectively in a co-design process, and how to implement change agents or security champions who push more towards effective patching than just mitigating measures. For the policy relevance, the documented challenges and barriers point to the need to complement binding, high-level mandates with soft-governance instruments (e.g. sector benchmarking of patch metrics and cooperation forums) so “timely” remediation is guided more and realistically achievable across organization sizes, not just large organizations.

7.8. Reflection on the Link to EPA Study Programme

Reflecting on the EPA programme, this research shows that software security patch management (SSPM) remains a complex governance issue that involves regulatory, technical, and social aspects. It addresses a key societal challenge: protecting digital infrastructure by improving how organizations patch software to prevent cyberattacks. SSPM is a wicked problem as it involves unclear responsibilities, trade-offs between speed and business continuity, and vague regulatory demands. This makes it a difficult policy issue. The use of semi-structured interviews and thematic analysis, as described in Chapter 4, yielded findings in Chapters 5 and 6, which showed how organizations struggle to implement regulations and how socio-technical factors interact with regulations. Regulation not only brings challenges and barriers for patch management, but also provides an opportunity for organizations to raise their security maturity and to harmonize this across sectors. This research reflects EPA’s emphasis on complex systems by showing how patching involves technical, human, regulatory and organizational facts, and how informal practices and decentralized structures influence decisions. Finally, the insights lead to practical policy advice for improving patching processes and guiding future development of patch management in Sections 7.4 and 7.5.

8

Conclusion

The goal of this research was to examine how organizations operationalize patch management under the growing influence of recent EU regulations, particularly DORA and NIS2, and how these regulations interact with the socio-technical factors that influence patching practices. A central objective was to explore not only the challenges organizations face in interpreting and implementing regulations into their patch management policies and processes, but also the barriers that arise within the day-to-day remediation process under regulatory pressure. Additionally, the research sought to look at the effects of non-prescriptive regulations (DORA/NIS2) on patching speed and reporting/documentation practices. To answer the following question, semi-structured interview data was collected from consultants and two case study organizations and further analyzed with inductive thematic analysis:

How do regulations influence organizations' patch management policies and practices, and how do socio-technical factors interact with these?

Critically, regulations have the potential to be both a catalyst and a constraint. On one hand, they can improve patching speed for large, critical organizations that have historically been exposed to regulation for a while, by raising the visibility of patch management to the executive level, increasing accountability for timely remediation, and embedding business risk perspectives into patching decisions. Prescriptive requirements, such as vulnerability scanning frequency, remediation timelines, escalation mechanisms, and documentation and reporting, structure the workflow end-to-end, shift key decisions upward to management functions, and often require the creation of coordinating functions (e.g., dedicated coordinators, maintenance groups, and response capacity).

On the other hand, in the initial phases newly regulated organizations first face the challenge of understanding and translating non-prescriptive mandates into workable policies and controls. Their progress in tackling these challenges typically depends on finding viable workarounds, such as co-designing workshops, iterative setting of risk-based timelines, and systematic mapping of regulatory requirements to internal standards and control frameworks, while navigating persistent socio-technical barriers (legacy complexity, unclear ownership, decentralized structure, limited automation, and cross-team coordination). The effectiveness of regulations therefore hinges on prior capabilities and on how deliberately large, critical organizations manage these barriers. When regulatory expectations are not aligned with the reality of patching, the pressure can create overhead without expanding an organization's capacity to address it. This misalignment widens the gap between compliance and resilience. Conversely, when capabilities exist within organizations, such as in previously regulated organizations, the same requirements can serve as a lever for more disciplined, risk-based patching.

This helps explain the difference in observed impact. For previously regulated organizations that have built capabilities over time, patching speed tends to increase and additional documentation does not introduce delay because processes, roles, and tools (e.g., ticketing and evidence capture) are already embedded. By contrast, newly regulated organizations, that often have to expand the scope of assets brought under regulations, experience documentation as overhead at first which causes delays and

reduces patching speed. This is precisely the case because the required processes and tooling are still being established. As these processes and capabilities mature and socio-technical barriers are actively managed, the regulatory burden shifts from friction to enabler, and the intended gains in timeliness and effectiveness become attainable.

Besides the strengths of this research's findings, this study has a few limitations. The study relied on semi-structured interviews, meaning findings are based on perceptions and views of participants. This introduces risks such as social desirability bias, selective recall, and potential underreporting of informal or non-compliant practices. The research also reflects a single point in time, and thus may not capture evolving patch management behaviors, especially considering the lack of use of quantitative data. Furthermore, at the time of the study, some regulations, such as NIS2 and BIO2, had not yet been transposed into national law, limiting the ability to assess their actual impact. As a result, some conclusions, particularly regarding NIS2, are anticipatory and based on organizational expectations rather than observed outcomes.

Future research should triangulate interview findings with additional data sources such as direct observation, system-level patching metrics or a combination of data from security information and event systems (SIEMs), CMDBs and ticketing tools to validate or challenge reported practices. Longitudinal studies could provide insights into how patching performance changes over time under sustained regulatory pressure. Further investigation will be needed once new regulations like NIS2 and BIO2 are fully implemented, which enable analysis of their real-world impact on (OT) patching timelines, governance, and patching behavior.

All in all, this research leads to several recommendations for both large, critical organizations and policymakers. For organizations, particularly those newly brought under regulations, adopting established practices and workarounds from mature, previously regulated large organizations can significantly ease the translation of regulatory requirements into patch and vulnerability management policies. By implementing these practices early, before new regulations such as NIS2 are fully transposed into national law, organizations can avoid the ”learning curve” delays and inefficiencies often seen during initial compliance phases. This means mapping legal requirements onto established frameworks (e.g., ISO/IEC 27002, CIS Controls), and applying structured scoping and classification by using DORA's criteria, for example. Crucially, policies should be co-designed with the people who have to live with them. That means early, genuine involvement of security, IT/OT operations, and business process owners; incorporating feedback rather than holding perfunctory “listening sessions”; and, where needed, softening timelines or differentiating policies (e.g., separate IT vs. OT patching rules) even if this adds some additional overhead. In parallel, organizations should move from box-ticking toward meaningful remediation, which means taking a risk-based approach that concentrates effort on the most critical known assets and exploitable vulnerabilities, preserves capacity for quick responses to emerging threats, and accepts practical limits. Perfect end-to-end automation, for example, is unrealistic and a perfectly complete CMDB is often unattainable, particularly in OT. Appointing security champions or change agents can also counter shallow “patch or mitigate” shortcuts and keep teams oriented towards effective patches.

For policymakers and regulators, the results highlight the value of supplementing binding legislation with forms of soft governance that foster learning and alignment within sectors. This includes creating cooperation forums and benchmarking systems to provide organizations with a clear understanding of how their patch management performance compares to peers. Though, the collection of data should be made possible for all kinds of organizations and sharing experiences should not be used to gain competitive advantage between firms. Such benchmarks and standards could then supplement current regulations with achievable, context-sensitive timelines, giving organizations both a defensible reference point for investment decisions and a clearer pathway to sustained compliance. To conclude, the surge in CVEs and increase in regulatory pressure will not slow, but by adopting proven workarounds and strategies, organizations can carry out timely and effective patching and turn regulatory pressure into cyber resilience.

References

Aalvik, H., Nguyen-Duc, A., Cruzes, D. S., & Iovan, M. (2023). Establishing a security champion in agile software teams: A systematic literature review [Series Title: Lecture Notes in Networks and Systems]. In K. Arai (Ed.), *Advances in information and communication* (pp. 796–810, Vol. 652). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-28073-3_53

Adebimpe Bolatito Ige, Eseoghene Kupa, & Oluwatosin Ilori. (2024). Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future. *GSC Advanced Research and Reviews*, *19*(3), 344–360. https://doi.org/10.30574/gscarr.2024.19.3.0236

Al-Ayed, A., Furnell, S., Zhao, D., & Dowland, P. (2005). An automated framework for managing security vulnerabilities. *Information Management and Computer Security*, *13*(2), 156–166. https://doi.org/10.1108/09685220510589334

Alhubaiti, O., & El-Alfy, E.-S. M. (2019). Impact of spectre/meltdown kernel patches on crypto-algorithms on windows platforms. *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 1–6. https://doi.org/10.1109/3ICT.2019.8910282

Andrew, C. (2005). The five ps of patch management: Is there a simple way for businesses to develop and deploy an advanced security patch management strategy? *Computers and Security*, *24*(5), 362–363. https://doi.org/10.1016/j.cose.2005.06.005

Avsuvarova, K. (2023). Navigating digital transformation: Unpacking the impact of DORA on the insurance landscape. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4549704

Barrett, R. (2004). People and policies: Transforming the human-computer partnership. *Proceedings. Fifth IEEE International Workshop on Policies for Distributed Systems and Networks, 2004. POLICY 2004.*, 111–114. https://doi.org/10.1109/POLICY.2004.1309157

Bauer, J., & Herder, P. (2009). Designing socio-technical systems. In D. Gabbay, A. Meijers, P. Thagard, & J. Woods (Eds.), *Handbook of the philosophy of science: Handbook philosophy of technology and engineering sciences* (pp. 601–631). Elsevier. https://doi.org/10.1016/B978-0-444-51667-1.50026-4

Beattie, S., Arnold, S., Cowan, C., Wagle, P., & Wright, C. (2002). Timing the application of security patches for optimal uptime. *LISA*, *2*, 233–242. https://www.usenix.org/conference/lisa-02/timing-application-security-patches-optimal-uptime

Bezzubov, D., Ihonin, R., & Diorditsa, I. (2017). Cyberthreats as a component of threats in the contemporary world (a legal aspect) [Number: 7]. *Journal of Advanced Research in Law and Economics*, *8*(7), 2086–2093. https://doi.org/10.14505/jarle.v8.7(29).04

Blackwell, R. W. N., Lowton, K., Robert, G., Grudzen, C., & Grocott, P. (2017). Using experience-based co-design with older patients, their families and staff to improve palliative care experiences in the emergency department: A reflective critique on the process and outcomes. *International Journal of Nursing Studies*, *68*, 83–94. https://doi.org/10.1016/j.ijnurstu.2017.01.002

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2022). Conceptual and design thinking for thematic analysis. *Qualitative Psychology*, *9*(1), 3–26. https://doi.org/10.1037/qup0000196

Braun, V., Clarke, V., Hayfield, N., & Terry, G. (2018). Thematic analysis. In P. Liamputtong (Ed.), *Handbook of research methods in health social sciences* (pp. 1–18). Springer Singapore. https://doi.org/10.1007/978-981-10-2779-6_103-1

Breakspear, S. (2012). *The policy impact of PISA: An exploration of the normative effects of international benchmarking in school system performance*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2012/02/the-policy-impact-of-pisa_g17a20ec/5k9fdfqffr28-en.pdf

Brykczynski, B., & Small, R. (2003). Reducing internet-based intrusions: Effective security patch management. *IEEE Software*, *20*(1), 50–57. https://doi.org/10.1109/MS.2003.1159029

Carr, M., & Lesniewska, F. (2020). Internet of things, cybersecurity and governing wicked problems: Learning from climate change governance. *International Relations*, *34*(3), 391–412. https://doi.org/10.1177/0047117820948247

Case, D. U. (2016). Analysis of the cyber attack on the ukrainian power grid. *3*(388), 1–29. Retrieved November 15, 2024, from https://www.vnf.com/webfiles/cyberattackukraine.pdf

Cavusoglu, H., & Jun, Z. (2008). Security patch management: Share the burden or share the damage? *Management Science*, *54*(4), 657–670. https://doi.org/10.1287/mnsc.1070.0794

Cavusoglu, H., Cavusoglu, H., & Zhang, J. (2006). Economics of security patch management. Retrieved December 8, 2024, from https://www.semanticscholar.org/paper/Economics-of-Security-Patch-Management-Cavusoglu-Cavusoglu/94e83e5b5fd375e2e3f226cfb15c2c8259c1651a

Center for Internet Security. (n.d.-a). CIS critical security controls version 8.1. https://www.cisecurity.org/controls/v8-1

Center for Internet Security. (n.d.-b). Patch management standard. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.cisecurity.org/-/media/project/cisecurity/cisecurity/data/media/files/uploads/2020/06/Patch-Management-Standard.docx&ved=2ahUKEwi6_NuVh9OOAxXk3gIHHVeVIbgQFnoECAkQAQ&usg=AOvVaw1Loyh4b8kdDhyxhikdH0E_

Centre for Information Security and Privacy Protection. (n.d.). *Baseline information security government*. Retrieved March 20, 2025, from https://www.cip-overheid.nl/producten-en-diensten/bio-tekst

Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from stuxnet. *Computer*, *44*(4), 91–93. https://doi.org/10.1109/MC.2011.115

Conry-murray, A. (2005). The evolution of patch management. *Network Magazine*, *20*(5), 43–47. https://www.scopus.com/inward/record.uri?eid=2-s2.0-18344367874&partnerID=40&md5=3224710c64eb35ed2124b2f60fc7c740

Cybersecurity & Infrastructure Security Agency. (2021). *BOD 22-01: Reducing the significant risk of known exploited vulnerabilities*. https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities

De Smale, S., Van Dijk, R., Bouwman, X., Van Der Ham, J., & Van Eeten, M. (2023). No one drinks from the firehose: How organizations filter and prioritize vulnerability information. *2023 IEEE Symposium on Security and Privacy (SP)*, 1980–1996. https://doi.org/10.1109/SP46215.2023.10179447

Dey, D., Lahiri, A., & Zhang, G. (2015). Optimal policies for security patch management. *INFORMS Journal on Computing*, *27*(3), 462–477. https://doi.org/10.1287/ijoc.2014.0638

Dietrich, C., Krombholz, K., Borgolte, K., & Fiebig, T. (2018). Investigating system operators' perspective on security misconfigurations. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 1272–1289. https://doi.org/10.1145/3243734.3243794

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. (2022a). An empirical study of automation in software security patch management. https://doi.org/10.1145/3551349.3556969

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. (2022b). Software security patch management - a systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, *144*. https://doi.org/10.1016/j.infsof.2021.106771

Dissanayake, N., Zahedi, M., Jayatilaka, A., & Babar, M. (2021). A grounded theory of the role of coordination in software security patch management, 793–805. https://doi.org/10.1145/3468264.3468595

Dissanayake, N., Zahedi, M., Jayatilaka, A., & Babar, M. (2022). Why, how and where of delays in software security patch management: An empirical investigation in the healthcare sector. *Proceedings of the ACM on Human-Computer Interaction*, *6*. https://doi.org/10.1145/3555087

Dryden, E. M., Anwar, C., Conti, J., Boudreau, J. H., Kennedy, M. A., Hung, W. W., Nearing, K. A., Pimentel, C. B., & Moo, L. (2024). The development and use of a new visual tool (REVISIT) to support participant recall: Web-based interview study among older adults. *JMIR Formative Research*, *8*, e52096. https://doi.org/10.2196/52096

Dutch Central Government. (2018, April 17). *Baseline Information Management Central Government* [Last Modified: 2023-07-12T15:42 Publisher: Ministerie van Onderwijs, Cultuur en Wetenschap]. Retrieved March 20, 2025, from https://www.informatiehuishouding.nl/documenten/richtlijnen/2018/05/01/baseline-informatiehuishouding-rijksoverheid

Erdődi, L., & Josang, A. (2020). Exploitation vs. prevention: The ongoing saga of software vulnerabilities. *Acta Polytechnica Hungarica*, *17*(7), 199–218. https://doi.org/10.12700/APH.17.7.2020.7.11

Eriksen-Jensen, M. (2013). Holding back the tidal wave of cybercrime. *Computer Fraud & Security*, *2013*(3), 10–16. https://doi.org/10.1016/S1361-3723(13)70028-9

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1. https://doi.org/10.11648/j.ajtas.20160501.11

European Banking Authority. (2019). *Guidelines on ICT and security risk management*. https://www.eba.europa.eu/sites/default/files/2025-02/23684f95-f669-4852-94a0-dac6c2ae67ad/Final%20report%20on%20amending%20GLs%20on%20ICT%20risk%20and%20security.pdf

European Banking Authority, European Insurance and Occupational Pensions Authority, & European Securities and Markets Authority. (2022). *Regulatory technical standards on ICT risk management framework and on simplified ICT risk management framework*. Retrieved March 20, 2025, from https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/regulatory-technical-standards-ict-risk-management-framework-and-simplified-ict-risk-management#activity-versions

European Network and Information Security Agency . (2013). *Window of exposure… a real problem for SCADA systems?: Recommendations for europe on SCADA patching.* Publications Office. Retrieved March 19, 2025, from https://data.europa.eu/doi/10.2824/25757

European Parliament. (2022). The NIS2 directive. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

European Union. (2022). *Digital operational resilience act*. Retrieved December 4, 2024, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

European Union Agency for Cybersecurity. (2020). *European cybersecurity certification scheme for cloud services*. Retrieved November 14, 2024, from https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

European Union Agency for Cybersecurity. (2021). *Cybersecurity guide for SMEs: 12 steps to securing your business*. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Cybersecurity%20guide%20for%20SMEs-online-single_page.pdf

Eyles, H., Jull, A., Dobson, R., Firestone, R., Whittaker, R., Te Morenga, L., Goodwin, D., & Mhurchu, C. N. (2016). Co-design of mHealth delivered interventions: A systematic review to assess key methods and processes. *Current Nutrition Reports*, *5*(3), 160–167. https://doi.org/10.1007/s13668-016-0165-7

Farr, M. (2018). Power dynamics and collaborative mechanisms in co-production and co-design processes. *Critical Social Policy*, *38*(4), 623–644. https://doi.org/10.1177/0261018317747444

Fletcher, K. (2023). The role of management decisions in creating cybersecurity vulnerabilities. *Issues in Information Systems*, *24*(2), 46–59. https://doi.org/10.48009/2_iis_2023_105

Furnell, S. (2016). Vulnerability management: Not a patch on where we should be? *Network Security*, *2016*(4), 5–9. https://doi.org/10.1016/S1353-4858(16)30036-8

Gamblin, J. (n.d.). *CVE data* [CVE.ICU]. Retrieved December 6, 2024, from https://cve.icu/CVEAll.html

Gentile, U., & Serio, L. (2019). Survey on international standards and best practices for patch management of complex industrial control systems: The critical infrastructure of particle accelerators case study. *International Journal of Critical Computer-Based Systems*, *9*(1), 115. https://doi.org/10.1504/IJCCBS.2019.098812

Gerace, T., & Cavusoglu, H. (2005). The critical elements of patch management, 98–101. https://doi.org/10.1145/1099435.1099457

Gerace, T., & Cavusoglu, H. (2009). The critical elements of the patch management process. *Communications of the ACM*, *52*(8), 117–121. https://doi.org/10.1145/1536616.1536646

Gerace, T., & Mouton, J. (2004). The challenges and successes of implementing an enterprise patch management solution, 30–33. https://doi.org/10.1145/1027802.1027810

Gooch, D., Price, B. A., Klis-Davies, A., & Webb, J. (2021). A design exploration of health-related community displays. *Proceedings of the ACM on Human-Computer Interaction*, *5*, 1–22. https://doi.org/10.1145/3449159

Goodin, D. (2017). Failure to patch two month old bug led to massive equifax breach. https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/

Grima, S., & Marano, P. (2021). Designing a model for testing the effectiveness of a regulation: The case of DORA for insurance undertakings. *Risks*, *9*(11), 206. https://doi.org/10.3390/risks9110206

Harrington, C. N., Wilcox, L., Connelly, K., Rogers, W., & Sanford, J. (2018). Designing health and fitness apps with older adults: Examining the value of experience-based co-design. *Proceedings of the 12th EAI International Conference on Pervasive Computing Technologies for Healthcare*, 15–24. https://doi.org/10.1145/3240925.3240929

Head, B. W., & Alford, J. (2015). Wicked problems: Implications for public policy and management. *Administration & Society*, *47*(6), 711–739. https://doi.org/10.1177/0095399713481601

Hoque, M. S., Jamil, N., Amin, N., & Lam, K.-Y. (2021). An improved vulnerability exploitation prediction model with novel cost function and custom trained word vector embedding. *Sensors*, *21*(12), 4220. https://doi.org/10.3390/s21124220

Hoque, M., Jamil, N., Amin, N., & Mansor, M. (2023). Risk-ranking matrix for security patching of exploitable vulnerabilities. *2808*. https://doi.org/10.1063/5.0134560

Hrebec, D. G., & Stiber, M. (2001). A survey of system administrator mental models and situation awareness. *Proceedings of the 2001 ACM SIGCPR conference on Computer personnel research*, 166–172. https://doi.org/10.1145/371209.371231

Hughes, C., & Robinson, N. (2024). *Effective vulnerability management: Managing risk in the vulnerable digital ecosystem*. 10.1002/9781394277155

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: A systematic mapping study. *Arabian Journal for Science and Engineering*, *45*(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

IEC. (2015). Security for industrial automation and control systems – part 2-3: Patch management in the IACS environment. Retrieved March 11, 2025, from https://webstore.iec.ch/en/publication/22811

ISO/IEC. (2013). ISO/IEC 27002:2013 information technology — security techniques — code of practice for information security controls. Retrieved March 11, 2025, from https://www.iso.org/standard/54533.html

ISO/IEC. (2022). ISO/IEC 27002:2022 information security, cybersecurity and privacy protection — information security controls. Retrieved March 11, 2025, from https://www.iso.org/standard/75652.html

Jaatun, M. G., & Soares Cruzes, D. (2021). Care and feeding of your security champion. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–7. https://doi.org/10.1109/CyberSA52016.2021.9478254

Jabin, M. (2024). Operational disruption in healthcare associated with software functionality issue due to software security patching: A case report. *Frontiers in Digital Health*, *6*. https://doi.org/10.3389/fdgth.2024.1367431

Jenkins, A. D. G., Liu, L., Wolters, M. K., & Vaniea, K. (2024). Not as easy as just update: Survey of system administrators and patching behaviours. *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 1–17. https://doi.org/10.1145/3613904.3642456

Kansal, Y., Kapur, P., & Sachdeva, N. (2019). Determining best patch management software using intuitionistic fuzzy sets with TOPSIS. *International Journal of Performability Engineering*, *15*(5), 1297–1305. https://doi.org/10.23940/ijpe.19.05.p5.12971305

Kansal, Y., Kumar, D., & Kapur, P. K. (2016). Vulnerability patch modeling. *International Journal of Reliability, Quality and Safety Engineering*, *23*(6), 1640013. https://doi.org/10.1142/S0218539316400131

Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, 4490–4494. https://doi.org/10.1109/IECON.2011.6120048

Kaur, K. (2020). A study of cyber security and cyber threats. *CGC International Journal of Contemporary Technology and Research*, *3*(1), 154–157. https://doi.org/10.46860/cgcijctr.2020.12.26.154

Kim, J., Sohn, M., & Won, Y. (2017). An automatic patch management system with improved security. *448*, 74–80. https://doi.org/10.1007/978-981-10-5041-1_13

Kim, J., & Won, Y. (2017). Patch integrity verification method using dual electronic signatures. *Journal of Information Processing Systems*, *13*(6), 1516–1526. https://doi.org/10.3745/JIPS.03.0084

Kim, Y., & Won, Y. (2020). A new cost-saving and efficient method for patch management using blockchain. *Journal of Supercomputing*, *76*(7), 5301–5319. https://doi.org/10.1007/s11227-019-02946-y

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering – a systematic literature review. *Information and Software Technology*, *51*(1), 7–15. https://doi.org/10.1016/j.infsof.2008.09.009

Kost, E. (2025). *10 biggest data breaches in finance* [Upguard]. Retrieved May 20, 2025, from https://www.upguard.com/blog/biggest-data-breaches-financial-services

Kotzias, P., Bilge, L., Vervier, P.-A., & Caballero, J. (2019). Mind your own business: A longitudinal study of threats and vulnerabilities in enterprises. *Proceedings 2019 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2019.23522

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, *38*(2), 143–154. https://doi.org/10.1016/j.apergo.2006.03.010

Li, F., Rogers, L., Mathur, A., Malkin, N., & Chetty, M. (2019). Keepers of the machines: Examining how system administrators manage software updates. https://doi.org/https://dl.acm.org/doi/10.5555/3361476.3361496

Li, X., Avellino, P., Janies, J., & Collins, M. P. (2016). Software asset analyzer: A system for detecting configuration anomalies. *MILCOM 2016 - 2016 IEEE Military Communications Conference*, 998–1003. https://doi.org/10.1109/MILCOM.2016.7795460

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Liu, S., Kuhn, R., & Rossman, H. (2009). Surviving insecure IT: Effective patch management. *IT Professional*, *11*(2), 49–51. https://doi.org/10.1109/MITP.2009.38

Lynch, K. (2021). *Cybersecurity is a global problem, so where's the global response?* [Forbes]. Retrieved November 15, 2024, from https://www.forbes.com/councils/forbestechcouncil/2021/05/20/cybersecurity-is-a-global-problem-so-wheres-the-global-response/

Maheshwari, D., & Janssen, M. (2014). Reconceptualizing measuring, benchmarking for improving interoperability in smart ecosystems: The effect of ubiquitous data and crowdsourcing. *Government Information Quarterly*, *31*, S84–S92. https://doi.org/10.1016/j.giq.2014.01.009

Malhotra, N., Zietsma, C., Morris, T., & Smets, M. (2021). Handling resistance to change when societal and workplace logics conflict. *Administrative Science Quarterly*, *66*(2), 475–520. https://doi.org/10.1177/0001839220962760

Markkanen, V., & Frantti, T. (2023). Patch management planning - towards one-to-one policy, 60–69. https://doi.org/10.1109/DSA59317.2023.00018

Marx, B., & Oosthuizen, D. (2016). Risk assessment and mitigation at the information technology companies. *Risk Governance and Control: Financial Markets and Institutions*, *6*(2), 44–51. https://doi.org/10.22495/rcgv6i2art6

Mehri, V. A., Arlos, P., & Casalicchio, E. (2023). Automated patch management: An empirical evaluation study. *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, 321–328. https://doi.org/10.1109/CSR57506.2023.10224970

Mell, P. M., Bergeron, T., & Henning, D. (2005). Creating a patch and vulnerability management program [Edition: 0]. https://doi.org/10.6028/NIST.SP.800-40ver2

Mell, P. M., & Tracy, M. C. (2002). Procedures for handling security patches [Edition: 0]. https://doi.org/10.6028/NIST.SP.800-40

Mileski, J., Clott, C., & Galvao, C. B. (2018). Cyberattacks on ships: A wicked problem approach. *Maritime Business Review*, *3*(4), 414–430. https://doi.org/10.1108/MABR-08-2018-0026

Min Khoo, H., & Robey, D. (2007). Deciding to upgrade packaged software: A comparative case study of motives, contingencies and dependencies. *European Journal of Information Systems*, *16*(5), 555–567. https://doi.org/10.1057/palgrave.ejis.3000704

Müller, R., Ruppert, J., Will, K., Wüsteney, L., & Heer, T. (2022). Analyzing the software patch discipline across different industries and countries. *P-323*, 159–170. https://doi.org/10.18420/sicherheit2022_10

National Cyber Security Centre. (2023a). *About CBW* [Last Modified: 2025-03-10T12:28 Publisher: Nationaal Cyber Security Centrum]. Retrieved March 20, 2025, from https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/samenvatting-nis2-richtlijn

National Cyber Security Centre. (2023b, November 6). *Duty of Care (Zorgplicht)* [Last Modified: 2025-03-17T10:59 Publisher: Nationaal Cyber Security Centrum]. Retrieved March 22, 2025, from https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/hoe-kan-uw-organiseren-zich-voorbereiden-op-de-nis2-richtlijn

Nicastro, F. (2007). Security patch management: The process [Journal Abbreviation: Information Security Management Handbook, Sixth Edition]. In *Information security management handbook, sixth edition* (pp. 185–200). https://www.scopus.com/inward/record.uri?eid=2-s2.0-85056545813&partnerID=40&md5=50d86beb37327ecfdb4919c69e5fcde5

Nunez, Y., Gustavson, F., Grossman, F., & Tappert, C. (2010). Designing a distributed patch management security system, 162–167. https://doi.org/10.1109/i-society16502.2010.6018816

Oberheide, J., Cooke, E., & Jahanian, F. (2009). If it ain't broke, don't fix it: Challenges and new directions for inferring the impact of software patches. *HotOS*. https://doi.org/https://dl.acm.org/doi/10.5555/1855568.1855585

Odumesi, J. O., & Sanusi, B. S. (2023). Achieving sustainable development goals from a cybersecurity perspective. *Advances in Multidisciplinary and scientific Research Journal Publication*, *2*(1), 1–10. https://doi.org/10.22624/AIMS/CSEAN-SMART2023P3

Paganini, P. (2025). *Air france and KLM warn of a data breach exposing customer data via unauthorized access to a third-party platform*. https://securityaffairs.com/180932/data-breach/air-france-and-klm-disclosed-data-breaches-following-the-hack-of-a-third-party-platform.html

Parchimowicz, K. (2024). Do not get lost in the cloud: How EU financial institutions could avoid problems with cloud services arising under DORA. *Law, Innovation and Technology*, *16*(2), 463–487. https://doi.org/10.1080/17579961.2024.2392935

PCI Security Standards Council. (2015). *PCI DSS quick reference guide: Understanding the payment card industry data security standard version 3.1*. https://listings.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf

Ponemon Institute. (2018). *Separating the truths from the myths in cybersecurity*. Retrieved November 20, 2024, from https://www.bmc.com/content/dam/bmc/collateral/third-party/Ponemon%2BReport.pdf

Prasad, R., & Rohokale, V. (2020). *Cyber threats and attack overview*. Retrieved November 19, 2024, from https://doi.org/10.1007/978-3-030-31703-4_2

Qiang, W., Liao, Y., Sun, G., Yang, L. T., Zou, D., & Jin, H. (2017). Patch-related vulnerability detection based on symbolic execution. *IEEE Access*, *5*, 20777–20784. https://doi.org/10.1109/ACCESS.2017.2676161

Rahman, M., Yan, G., Madhyastha, H., Faloutsos, M., Eidenbenz, S., & Fisk, M. (2013). iDispatcher: A unified platform for secure planet-scale information dissemination. *Peer-to-Peer Networking and Applications*, *6*(1), 46–60. https://doi.org/10.1007/s12083-012-0128-8

Rittel, H., & Webber, M. (1973). Dilemmas in a general theory of planning. https://urbanpolicy.net/wp-content/uploads/2015/06/Rittel-Webber_1973_DilemmasInAGeneralTheoryOfPlanning.pdf

Saunders, B., Kitzinger, J., & Kitzinger, C. (2015). Anonymising interview data: Challenges and compromise in practice. *Qualitative Research*, *15*(5), 616–632. https://doi.org/10.1177/1468794114550439

Schellong, A. R. (2010). Benchmarking EU e□government at the crossroads: A framework for e□government benchmark design and improvement. *Transforming Government: People, Process and Policy*, *4*(4), 365–385. https://doi.org/10.1108/17506161011081336

Schweizer, A., Lesage, S., & Gilles, I. (2017). Innovative way of analysing qualitative data: The combined use of lexicometric and thematic analyses. *The European health psychologist*, *19*, 566. https://api.semanticscholar.org/CorpusID:64545163

Seng, J.-L., Ko, I.-F., & Lin, B. (2009). A generic construct based workload model for web search. *Information Processing & Management*, *45*(5), 529–554. https://doi.org/10.1016/j.ipm.2009.04.004

ServiceNow & Ponemon Institute. (2020). *Costs and consequences of gaps in vulnerability response*. https://media.bitpipe.com/io_15x/io_152272/item_2184126/ponemon-state-of-vulnerability-response-.pdf

Shostack, A. (2003). Quantifying patch management. *Secure Business Quarterly*, *3*(2), 1–4. https://shostack.org/files/essays/sbq_patch_adam-shostack.pdf

Silva-Castañeda, L. (2016). In the shadow of benchmarks. normative and ontological issues in the governance of land. *Environment and Planning A: Economy and Space*, *48*(4), 681–698. https://doi.org/10.1177/0308518X15615767

Society for Worldwide Interbank Financial Telecommunications. (2025). *Customer security controls framework*. https://www2.swift.com/knowledgecentre/rest/v1/publications/cscf_dd/66.0/CSCF_v2026_202507015.pdf?logDownload=true

Souppaya, M., & Scarfone, K. (2013, July). *Guide to enterprise patch management technologies* (NIST SP 800-40r3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-40r3

Souppaya, M., & Scarfone, K. (2022, April 6). *Guide to enterprise patch management planning : Preventive maintenance for technology* (NIST SP 800-40r4). National Institute of Standards and Technology (U.S.) Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-40r4

ten Napel, G., Eeten, M. v., & Parkin, S. (2024). Speedrunning the maze: Meeting regulatory patching deadlines in a large enterprise environment [ISSN: 2375-1207], 81–81. https://doi.org/10.1109/SP61157.2025.00081

Tiefenau, C., Häring, M., Krombholz, K., & Von Zezschwitz, E. (2020). Security, availability, and multiple information sources: Exploring update behavior of system administrators. *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*, 239–258. https://doi.org/https://dl.acm.org/doi/10.5555/3488905.3488919

Trainor, L. R., & Bundon, A. (2021). Developing the craft: Reflexive accounts of doing reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, *13*(5), 705–726. https://doi.org/10.1080/2159676X.2020.1840423

Tyali, S., & Pottas, D. (2010). Information security management systems in the healthcare context. *Proceedings of the South African Information Security Multi-Conference: Port Elizabeth, South Africa, 17-18 May 2010*, 177–187. https://api.semanticscholar.org/CorpusID:16320585

Ujjwal Rao. (2023). Overview of cyber security. *International Journal of Advanced Research in Science, Communication and Technology*, 47–51. https://doi.org/10.48175/IJARSCT-9470

UNDP & ITU. (2023). *SDG digital acceleration agenda*. Retrieved November 14, 2024, from https://www.undp.org/sites/g/files/zskgke326/files/2023-09/SDG%20Digital%20Acceleration%20Agenda_2.pdf

van Engelen, Y. (2022). Exploring the practice of organisational security patch management from a socio-technical perspective. http://resolver.tudelft.nl/uuid:6d71f8a8-9941-4d57-bedb-8b3fb8c841e9

Van Den Berg, J., Van Zoggel, J., Snels, M., van Leeuwen, M., Boekee, S., Koppen, L., van den Berg, B., de Bos, A., & van der Lubbe, J. (2014). On (the emergence of) cyber security science and its challenges for cyber security education. Retrieved November 19, 2024, from https://www.semanticscholar.org/paper/On-(-the-Emergence-of-)-Cyber-Security-Science-and/f96e9e707341baf4eb2784a21cd95b33c41ab685

Vitale, F., McGrenere, J., Tabard, A., Beaudouin-Lafon, M., & Mackay, W. E. (2017). High costs and small benefits: A field study of how users experience operating system upgrades. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 4242–4253. https://doi.org/10.1145/3025453.3025509

Weber, E. P., & Khademian, A. M. (2008). Wicked problems, knowledge challenges, and collaborative capacity builders in network settings. *Public Administration Review*, *68*(2), 334–349. https://doi.org/10.1111/j.1540-6210.2007.00866.x

Yin, R. K. (2003). *Applications of case study research*. Sage publications. https://books.google.nl/books?hl=en&lr=&id=LM5yAwAAQBAJ&oi=fnd&pg=PP1&dq=Yin,+R.+K.+(2003).+Applications+of+case+study+research.+Sage+publications.+doi&ots=UJIHB4gOpG&sig=LQXZp59D3VIe05nW61fFH4dviTI

Zhu, Q., McQueen, M., Rieger, C., & Basar, T. (2011). Management of control system information security: Control system patch management. https://inldigitallibrary.inl.gov/sites/sti/sti/5025983.pdf

A

Publications Included in Literature Review

Table 4: Studies included in Literature Review

#	Title	Reference
1	Economics of Security Patch Management	(Cavusoglu et al., 2006)
2	Effective Vulnerability Management: Managing Risk in the Vulnerable Digital Ecosystem	(Hughes & Robinson, 2024)
3	The challenges and successes of implementing an enterprise patch management solution	(Gerace & Mouton, 2004)
4	An automatic patch management system with improved security	(J. Kim et al., 2017)
5	A new cost-saving and efficient method for patch management using blockchain	(Y. Kim & Won, 2020)
6	Not as easy as just update: Survey of System Administrators and Patching Behaviours	(Jenkins et al., 2024)
7	Risk-ranking matrix for security patching of exploitable vulnerabilities	(M. Hoque et al., 2023)
8	iDispatcher: A unified platform for secure planet-scale information dissemination	(Rahman et al., 2013)
9	An automated framework for managing security vulnerabilities	(Al-Ayed et al., 2005)
10	Reducing internet-based intrusions: Effective security patch management	(Brykczynski & Small, 2003)
11	The evolution of patch management	(Conry-murray, 2005)
12	Risk assessment and mitigation at the information technology companies	(Marx & Oosthuizen, 2016)
13	Operational disruption in healthcare associated with software functionality issue due to software security patching: a case report	(Jabin, 2024)
14	Optimal policies for security patch management	(Dey et al., 2015)
15	Patch integrity verification method using dual electronic signatures	(J. Kim & Won, 2017)
16	Designing a distributed patch management security system	(Nunez et al., 2010)
17	Security patch management: The process	(Nicastro, 2007)

Continued on next page

Table 4 – continued from previous page

#	Title	Reference
18	Analyzing the Software Patch Discipline Across Different Industries and Countries	(Müller et al., 2022)
19	Surviving insecure IT: Effective patch management	(Liu et al., 2009)
20	The five Ps of patch management: Is there a simple way for businesses to develop and deploy an advanced security patch management strategy?	(Andrew, 2005)
21	Security patch management: Share the burden or share the damage?	(Cavusoglu & Jun, 2008)
22	Determining best patch management software using intuitionistic fuzzy sets with TOPSIS	(Kansal et al., 2019)
23	Why, How and Where of Delays in Software Security Patch Management: An Empirical Investigation in the Healthcare Sector	(Dissanayake, Jayatilaka, et al., 2022a)
24	The critical elements of patch management	(Gerace & Cavusoglu, 2005)
25	A grounded theory of the role of coordination in software security patch management	(Dissanayake et al., 2021)
26	The role of management decisions in creating cybersecurity vulnerabilities	(Fletcher, 2023)
27	Software security patch management - A systematic literature review of challenges, approaches, tools and practices	(Dissanayake, Jayatilaka, et al., 2022b)
28	The critical elements of the patch management process	(Gerace & Cavusoglu, 2009)
29	An Empirical Study of Automation in Software Security Patch Management	(Dissanayake, Jayatilaka, et al., 2022a)
30	Patch management planning - towards one-to-one policy	(Markkanen & Frantti, 2023)
31	Vulnerability management: Not a patch on where we should be?	(Furnell, 2016)
32	Mind Your Own Business: A Longitudinal Study of Threats and Vulnerabilities in Enterprises	(Kotzias et al., 2019)
33	Speedrunning the Maze: Meeting Regulatory Patching Deadlines in a Large Enterprise Environment	(ten Napel et al., 2024)

Table 5: Standards included in Literature review

Year	Publication	Authors & Reference	Title of Publication
2002	NIST Special Publication (SP) 800-40	(Mell & Tracy, 2002)	Procedures for Handling Security Patches: Recommendations of the National Institute of Standards and Technology
2005	NIST Special Publication (SP) 800-40 Version 2	(Mell et al., 2005)	Creating a Patch and Vulnerability Management Program.
2013	NIST Special Publication (SP) 800-40 Revision 3	(Souppaya & Scarfone, 2013)	Guide to Enterprise Patch Management Technologies.
2013	ISO27002:2013	(ISO/IEC, 2013)	Information security, cybersecurity and privacy protection — Information security controls
2015	IEC TR 62443-2-3:2015	(IEC, 2015)	Security for Industrial Automation and Control Systems – Part 2-3: Patch Management in the IACS Environment
2022	ISO27002:2022	(ISO/IEC, 2022)	Information security, cybersecurity and privacy protection — Information security controls
2022	NIST Special Publication (SP) 800-40 Revision 4	(Souppaya & Scarfone, 2022)	Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology

B

Socio-technical challenges and factors in SSPM

B.1. Socio-technical Challenges and Coping Strategies

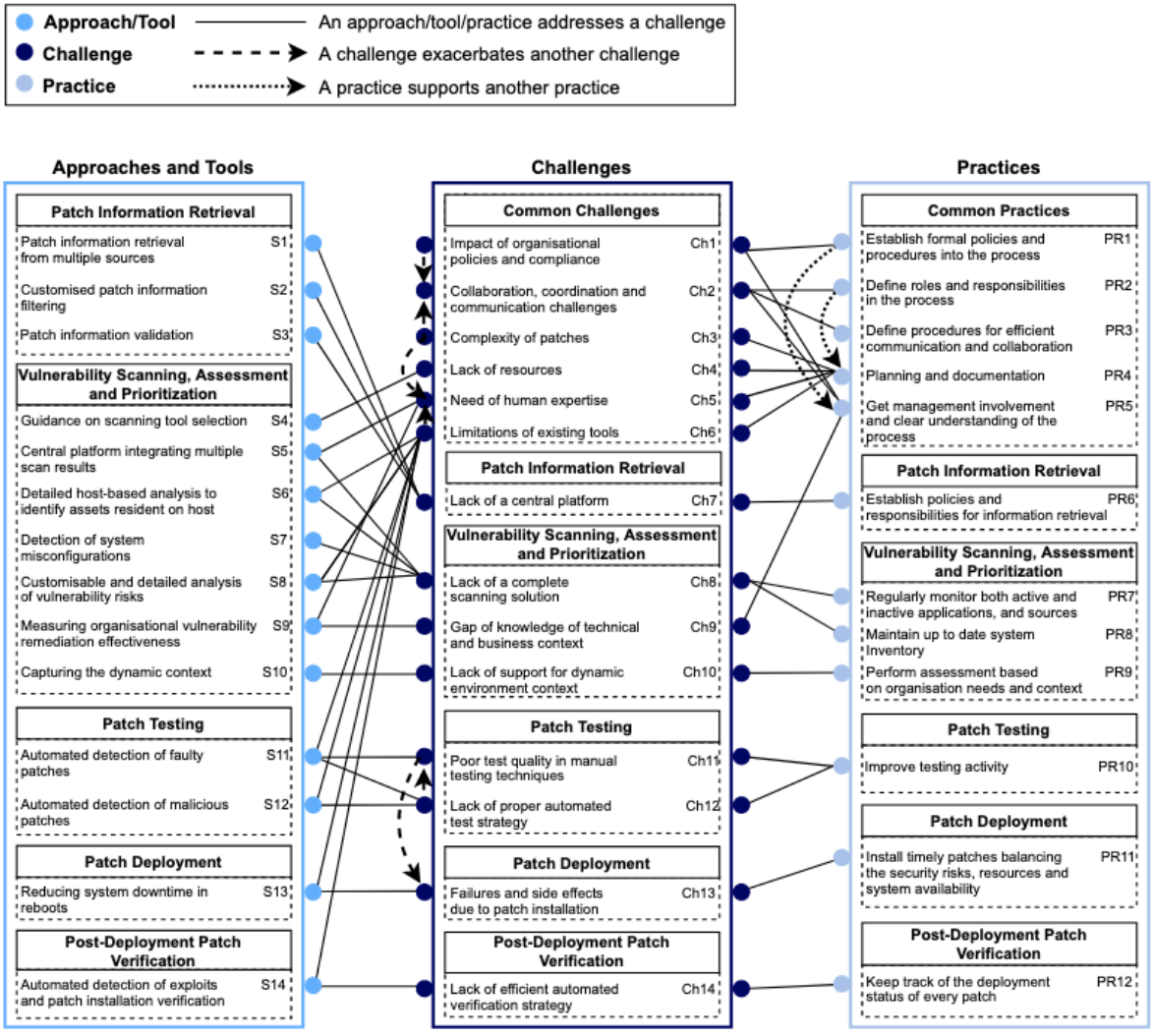

Figure 9: A mapping of challenges onto solutions by Dissanayake, Jayatilaka, et al. (2022b).

B.2. Socio-technical factors in SSPM

Category	Challenge	Factors	Type	Aspect	Decision
Organisational	**CO1** Developments of threat environment	**[F1]** Decreasing timeframe between vulnerability awareness and exploit by threat actor	Cause	Security	Time
		[F2] Unpredictability of vulnerability exploit	Cause	Security	Time
	CO2 Behaviour and awareness of system-owners[4]	**[F3]** Lack of threat perception of system-owners	Barrier	Security	Patch
		[F4] Lack of perception that patching reduces threat of system-owners	Barrier	Security	Patch
		[F5] Lack of knowledge how to patch of system-owners	Barrier	Operational	Time
		[F6] Lack of prioritization of system-owners	Barrier	Operational	Time
	CO3 Role and capability of IT practitioners	**[F7]** Human error during patch deployment of IT practitioners	Cause	Operational	Patch
		[F8] Human error in patch assessment of IT practitioners	Cause	Applicability	Patch
		[F9] Need for balance between patching and tasks of day-to-day job of IT practitioners	Constraint	Operational	Time
	CO4 Lack of human resources	**[F10]** Lack of human capacity of IT practitioners limits the frequency of patch deployment	Constraint	Operational	Time
	CO5 Organisational structure	**[F11]** Decentralized and large organisational structure	Cause	Applicability	Patch, Time
		[F12] Need to balance security practises and organisational objectives	Constraint	Availability, Security	Time
Procedural	**CP6** Collaboration	**[F13]** Inter-dependencies of different teams (e.g., Security, Systems, Quality) within the IT department	Barrier	Operational	Time
		[F14] Dependency of external stakeholders (e.g., end-users) to determine moment of patch event for central IT services	Barrier	Availability	Time
		[F15] Dependency of external stakeholders (e.g., system-owners) to patch their own systems	Barrier	Security	Patch
		[F16] Decision-making through multiple levels of the organisation	Barrier	Operational	Time
		[F17] Need for certainty about responsibility and accountability for IT department and system-owners	Barrier	Operational	Time
	CP7 Communication	**[F18]** Inter-dependencies of different teams regarding time of patch event	Barrier	Operational	Time
		[F19] Dependency of external stakeholders (e.g., vendors, experts, media) as information source for vulnerability notification, patch criticality level, patch availability	Cause	Security	Patch, Time
	CP8 Coordination	**[F20]** Responsibilities and authority of decision-making within IT department (inter-team)	Barrier	Operational, Security	Time
		[F21] Responsibilities and authority of decision-making of IT department within organisation	Barrier	Availability, Security	Time
		[F22] Lack of centrally arranged patch information retrieval	Barrier	Operational	Time
	CP9 Procedures and guidelines	**[F23]** Lack of availability of information throughout patching process for central IT services	Cause	Operational	Time
		[F24] Lack of KPI's to indicate effectiveness of patch process	Cause	Security	Time
		[F25] Organisational restrictions of available patch moments (e.g., change weekends)	Constraint	Availability	Time
		[F26] Lack of defined process for patching of non-central IT services	Cause	Security	Patch
		[F27] Lack of clarity and standardization of emergency-response procedure	Cause	Operational	Time
Technical	**CT10** Patch quality	**[F28]** Side-effects of patch deployment can harm system's functioning	Cause	Operational	Patch
		[F29] Emergency patch often lacks proper testing by vendor due to hurry of release	Cause	Operational	Patch
	CT11 Patch availability	**[F30]** No patch available by vendor (zero-day vulnerabilities)	Cause	Operational	Patch
		[F31] No patch available by open-source software usage	Cause	Operational	Patch
	CT12 System dependencies	**[F32]** Lack of knowledge of system dependencies (e.g. layers, versions)	Cause	Applicability	Patch, Time
		[F33] Known dependencies of applications and databases of servers and networks (e.g., layers and stacks)	Barrier	Operational	Patch, Time
	CT13 Technical (hardware) resources	**[F34]** Hardware capacity limits frequency of patch deployment	Constraint	Operational	Time
		[F35] Large magnitude of patch releases	Cause	Operational	Time
	CT14 Complexity of systems	**[F36]** Large number of unique servers that all need different patches, applied manually	Cause	Operational	Time
		[F37] Large number of legacy systems that are 'unpatchable'	Cause	Applicability	Patch
		[F38] Lack of knowledge of functioning and criticality of certain systems	Cause	Applicability	Patch
	CT15 Usage of automation tools	**[F39]** Lack of integrated automation tool usage throughout phases of patch process	Cause	Operational	Time
		[F40] Need for 'human-in-the-loop' to assess applicability and relevance of patch release	Constraint	Operational	Time
	CT16 Asset overview	**[F41]** Lack of complete overview of assets	Cause	Applicability	Time
		[F42] Lack of complete information of known assets (e.g., owner, patch status)	Cause	Applicability	Time
		[F43] Dependency of departments in knowledge of change of system owners	Cause	Applicability	Time

Figure 10: Challenges and socio-technical factors of security patching by van Engelen (2022).

C

Interview Questions

C.1. Introduction

- How long have you been working here for, and what is your role now?
- What is your role in security patching and vulnerability management?
- How much of your work involves security patching?

C.2. Patch Policy

- How is the severity or urgency of vulnerabilities assessed or categorized within your organization?
- How are decisions made about which vulnerabilities to prioritize for security patching, and how quickly they should be addressed? What factors are considered when prioritizing vulnerabilities relative to each other?
  - Probe: Is there an internal policy or framework that guides how vulnerabilities are classified and prioritized for patching?
  - Probe: How are patching timelines or deadlines determined for different severity levels in your policy? Do you rely on the ISO27002 or best practice standards like CISA's KEV timelines?
  - How do patching timelines differ for emergencies and highly critical vulnerabilities? Do the timelines always differ for highly critical vulnerabilities?
  - Probe: What guides this internal policy (e.g. regulation) and who is responsible for this internal policy?
  - Probe: Did you have patching policies pre-DORA/NIS2?

C.3. Information Retrieval

- How do you typically become aware and maintain awareness of vulnerabilities that need patching?
  - Probe: What trustworthy information resources do you use and update to build and maintain awareness about vulnerabilities?

C.4. Regulatory Expectations

- If regulation is what guides this internal policy, what are the regulatory expectations related to patch management?
  - Probe: Have NIS2/DORA led to any changes in your organization's patch management policies or standards? If so, what were they? How have they changed (if at all) since?
  - Probe: Have DORA or NIS2 had any noticeable impact on your patching workflows? If so, what impact?

  - Probe: Ever since the introduction of NIS2/DORA, has your approach to patch management changed? What challenges (related to information retrieval, scanning testing deployment and patch verification), if any, has your organization faced in aligning patch management practices with these EU regulations? [Then summarize each challenge that the participant mentions, and ask if there are others until they cannot think of any other challenge]
  - Are you under pressure to prove that your patching speed/frequency is ”reasonable”?;
  - Probe: Do regulations require you to document you patching practices more?
    * Probe: How are you expected to demonstrate continuous assurance and compliance (e.g. through documentation)?
    * Probe: What kind of documentation (e.g. logs, tickets, metrics, reports) is kept to demonstrate compliance with DORA/NIS2 patching expectations? How does your organization demonstrate continuous compliance with patching expectations under NIS2/DORA (e.g., logs, reports, metrics)?
    * Probe: How do DORA/NIS2 influence your documentation or reporting around patching?
    * Probe: Do regulations such as the NIS2/DORA cause delay in patching (e.g. due to administrative burden of documentation)?
  - Probe: Are you expected to notify the regulatory bodies about patches specifically?
    * Probe: If so, within what timeframe, and what do you need to report exactly (related to patches)?

C.5. Factors influencing patching speed

- What factors influence how quickly a patch is applied?;
- What are the biggest blockers to fast patch deployment?
  - Probe: Are there risks or constraints (e.g., system stability, downtime windows) that delay patching?
  - Probe: From a technical or organizational perspective, do regulations such as the NIS2/DORA cause delay in patching?
  - Probe: Has your patching speed improved, worsened, or stayed the same due to increasing regulatory expectations?

C.6. Emergency and escalation procedures

- How often are patches delayed and how are these delayed patches tracked and reviewed?
  - Probe: How do you ensure that patching decisions are still timely in the absence of explicit deadlines imposed by regulations?
  - Probe: Are you under pressure to prove that your patching speed/frequency is ”reasonable” according to the regulation? How is that determined?
- How are exceptions to patching policies handled (e.g., when a patch cannot be applied in time)?
  - Probe: Is there a formal process for documenting and approving exceptions?
  - Probe: Which risk assessments or compensating controls are used in such cases?
- When does a critical vulnerability lead to an escalation and/or emergency, and is that always the case (e.g. for exceptions)?
- Is there a clear escalation process for critical vulnerabilities?
  - Probe: Who decides what qualifies as critical?
  - Probe: How do emergency patches and escalations differ in process or urgency under DORA/NIS2?
  - Probe: Do you ever mention/refer to regulatory expectations when prioritizing patches?

C.7. Overall Experience and Future Developments

- What (regulatory) developments do you see for patch management in the future?
  - Probe: Taking a broader perspective, from your experience, does the approach by NIS2/DORA ensure patch management is improved?
  - Probe: Are there future plans to adapt or further evolve your patching policies in anticipation of audits, supervision, or maturing interpretations of the regulations?

D

Informed Consent Form Interviews

Opening Statement - Interviews

You are being invited to participate in a research study titled ”Addressing Socio-Technical Challenges in Software Security Patch Management.” This study is being conducted by Nikhil Daswani from TU Delft as part of a Thesis Internship at Accenture.

The purpose of this research study is to the impact of EU legislation, and human, organizational and technical factors on the effectiveness and timeliness of Software Security Patch Management (SSPM). This study will take approximately 45-60 minutes to complete. The data collected will be used for academic publication and policy recommendations.

We will be asking you to participate in a structured study involving interviews, where you will provide insights on the key (regulatory) challenges, decision-making processes, and best practices in SSPM within your industry or area of expertise.

For the administrative purposes, your contact details including your name and e-mail address will be recorded. To maintain validity of the gained insights from the interviews, your job description and domain expertise will also be recorded. Finally, a recording and transcription will be made by the interviewer/ organizer of the meeting through TU Delft MS Teams for research purposes. None of the data will be made public and will only be accessible to the research team at TU Delft (see researchers mentioned below). Your insight will be combined with the insights of other experts in the field and will be reported in an aggregated and anonymous manner in a MSc thesis report. Only anonymous quotes will be used in the report. The data may be reused for future scientific and education activities within TU Delft on the topic of Patch Management. You will be anonymous in any and all outputs.

As with any online activity, the risk of a breach is always possible. To the best of our ability, your answers in this study will remain confidential. We will minimize any risks by ensuring that personally identifiable information (PII) such as names, email addresses, or IP addresses will be stored at TU Delft. All responses will be accessible only to authorized researchers (see below). The collected data will be stored for up to 2 years. However, all personal data will be deleted at the latest (approximate date: November 2027).

This study follows Open Data principles. An anonymized version of the dataset may be shared for academic transparency and future research, ensuring that no identifiable information is disclosed.

Your participation in this study is entirely voluntary, and you can withdraw at any time. You are free to omit any questions. Since the interview is not anonymous, it will be possible to remove recordings once they have been recorded. After the interview is done, we will send you the transcript for review. Should you have any concerns regarding its content, feel free to suggest changes/modifications.

By signing below you agree to participate in this study.

Signatures
I accurately read the consent form as a potential participant, and I have had the opportunity to ask questions. I understand what I am giving consent for and I confirm that I am giving consent freely.

_____	_____	_____
Name of participant [printed]	Signature	Date

E

Mapping of Legislation to Standards to CIS Controls Framework

This Appendix presents a structured mapping of the key regulatory requirements found in BIO, DORA, and NIS2 (CBW) to relevant information security standards (e.g., ISO 27002) and control frameworks (e.g., CIS Controls). To make the mapping more interpretable, individual statements from the publications were analyzed per phase of the patch management process (as described by Dissanayake, Jayatilaka, et al. (2022b)) and grouped under broader aspects. These aspects are thematic categories that reflect the nature or focus of the requirement. For example, several statements across different standards that relate to sources of information for information retrieval were consolidated under the aspect “Information Sources” in Appendix E.1. These aspects were inductively derived during the mapping process by identifying recurring patterns and shared objectives among statements. The approach ensures that the mapping does not remain a fragmented list of requirements, but instead highlights the themes that help organizations translate different regulatory inputs into coherent patch management policies and procedures.

E.1. Information Retrieval

Table 6: Mapping for Information Retrieval

Type	Aspect	Publication	Section	Guideline / Requirement
Regulations	Information Sources	(European Banking Authority et al., 2022)	10.2.a	Identify and update relevant and trustworthy information resources to build and maintain awareness about vulnerabilities.
Standards	Techniques for Information Retrieval	(Mell & Tracy, 2002)	–	The patching and vulnerability policy should specify what techniques an organization will use to monitor for new patches and vulnerabilities and which personnel will be responsible for such monitoring.
		(Souppaya & Scarfone, 2013)	4.1	Organizations should carefully consider the advantages and disadvantages of each technique for identifying missing patches (e.g., agent-based, agentless scanning, passive network monitoring) when selecting enterprise patch management technologies.
	Information Sources	(Mell et al., 2005)	–	Monitor security sources for vulnerability announcements, patch and non-patch methods of remediation, and emerging threats that match up with the software within the system inventory of the PVG.
		(Center for Internet Security, n.d.-b)	4.0.3	A process must be in place to manage patches. This process must include the following: monitoring security sources (Appendix A) for vulnerabilities, patch and non-patch remediation, and emerging threats.

Continued on next page

Table 6 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
Standards		(ISO/IEC, 2013)	12.6.1	Information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology; these information resources should be updated based on changes in the inventory or when other new or useful resources are found.
		(Souppaya & Scarfone, 2022)	2.2.1	For example, your organization might subscribe to vulnerability feeds from software vendors, security researchers, and the National Vulnerability Database (NVD).
		(ISO/IEC, 2022)	5.6	Membership of special interest groups or forums should be considered as a means to: a) improve knowledge about best practices and stay up to date with relevant security information; b) ensure the understanding of the information security environment is current; c) receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities; d) gain access to specialist information security advice; e) share and exchange information about new technologies, products, services, threats or vulnerabilities; f) provide suitable liaison points when dealing with information security incidents (see 5.24 to 5.28).
		(ISO/IEC, 2022)	8.6	To identify technical vulnerabilities, the organization should consider: for software and other technologies (based on the asset inventory list, see 5.9), identifying information resources that will be used for identifying relevant technical vulnerabilities and maintaining awareness about them. Updating the list of information resources based on changes in the inventory or when other new or useful resources are found.
	Timeliness of Information Retrieval	(ISO/IEC, 2013)	12.6.1	Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
		(ISO/IEC, 2013)	12.6.1	A timeline should be defined to react to notifications of potentially relevant technical vulnerabilities.
Control Framework	Information Sources	(Center for Internet Security, n.d.-a)	Control 17; Safeguard 17.2	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.
			Control 17; Safeguard 17.2	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.

E.2. Vulnerability Scanning, Assessment & Prioritization

Table 7: Mapping for Vulnerability Scanning, Assessment & Prioritisation

Type	Aspect	Publication	Section	Guideline / Requirement
Regulations	Risk Assessment	(European Parliament, 2022)	21.g	Ensure Cyber Hygiene is in Order: basic practices for cyber hygiene and cybersecurity training: To increase organizations' cybersecurity resilience, start with a risk analysis. An important next step is to implement basic cyber hygiene practices. Training employees to adhere to these basic practices is essential for the resilience of an organization.
		(National Cyber Security Centre, 2023b)	5	Perform a risk analysis: Performing a risk analysis is the first step in improving the cybersecurity resilience of your company or organization. It is a crucial first step in gaining the necessary insights. A risk analysis reveals which risks are the most significant and where security measures are most needed.
		(Dutch Central Government, 2018)	12.6	If a patch is available, all associated risks must be assessed, comparing the risk of the vulnerability to the risk of installing the patch.
		(Dutch Central Government, 2018)	12.6	It is advised to retain previous scan reports to facilitate the identification of differences. At a minimum, this should be done for the most critical systems. Any changes in systems, such as open network ports or newly added services, must be examined.
		(European Banking Authority et al., 2022)	8.3	Financial entities, other than microenterprises, shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems and, in any case before and after connecting technologies, applications or systems.
		(European Banking Authority et al., 2022)	8.7	Financial entities, other than microenterprises, shall perform a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their ICT supported business functions, information assets or ICT assets
	Vulnerability Scanning	(European Banking Authority et al., 2022)	10.2.b	ensure the performance of automated vulnerability scanning and assessments on ICT assets, whereby the frequency and scope of those activities shall be commensurate to the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554 and the overall risk profile of the ICT asset; For the purposes of point (b), financial entities shall perform the automated vulnerability scanning and assessments on ICT assets for the ICT assets supporting critical or important functions on at least a weekly basis.
	Prioritization	(European Banking Authority et al., 2022)	10.2.f	prioritise the deployment of patches and other mitigation measures to address the vulnerabilities identified; For the purposes of point (f), financial entities shall consider the criticality of the vulnerability, the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554, and the risk profile of the ICT assets affected by the identified vulnerabilities.
Standards	Risk Assessment	(ISO/IEC, 2013)	12.6.1	Once a potential technical vulnerability has been identified, the organization should identify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems or applying other controls; (ISO/IEC, 2013) section 12.6.1
		(ISO/IEC, 2013)	12.6.1	If a patch is available from a legitimate source, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch);
		(Souppaya & Scarfone, 2022)	2.2.2	Plan the risk response. This involves assessing the risk the vulnerability poses to your organization, choosing which form of risk response (or combination of forms) to use, and deciding how to implement the risk response. For example, you might determine that risk is elevated because the vulnerability is present in many organization assets and is being exploited in the wild, then choose mitigation as the risk response and mitigate the vulnerability by upgrading the vulnerable software and altering the software's configuration settings. (Souppaya & Scarfone, 2022)
		(ISO/IEC, 2022)	8.8	To identify technical vulnerabilities, the organization should consider: conducting planned, documented and repeatable penetration tests or vulnerability assessments by competent and authorized persons to support the identification of vulnerabilities. Exercising caution as such activities can lead to a compromise of the security of the system;

Continued on next page

Table 7 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
Standards		(ISO/IEC, 2022)	8.8	To evaluate identified technical vulnerabilities, the following guidance should be considered: once a potential technical vulnerability has been identified, identifying the associated risks and the actions to be taken. Such actions can involve updating vulnerable systems or applying other controls.
	Prioritization	(Mell & Tracy, 2002)	-	An organization's patching process should define a method for deciding which systems get patched and which patches get installed first
		(Mell et al., 2005)	-	Prioritize the order in which the organization addresses the remediation of vulnerabilities, based on analysis of risks to systems.
		(Center for Internet Security, n.d.-b)	4.0.6	Patch management must be prioritized based on the severity of the vulnerability the patch addresses. In most cases, severity ratings are based on the Common Vulnerability Scoring System (CVSS). A CVSS score of 7-10 is considered a high impact vulnerability, a CVSS score of 4-6.9 is considered a moderate impact vulnerability and a CVSS of 0-3.9 is considered a low impact vulnerability.
		(ISO/IEC, 2013)	12.6.1	Systems at high risk should be addressed first; (ISO/IEC, 2013) section 12.6.1
		(Souppaya & Scarfone, 2022)	2.3.1	Prioritize the patch. A patch may be a higher priority to deploy than others because its deployment would reduce cybersecurity risk more than other patches would. Another patch may be a lower priority because it addresses a low-risk vulnerability on a small number of low-importance assets. (Souppaya & Scarfone, 2022)
		(ISO/IEC, 2022)	8.8	The following guidance should be considered to address technical vulnerabilities: addressing systems at high risk first;
	Procedures	(ISO/IEC, 2013)	12.6.1	Depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management (see 12.1.2) or by following information security incident response procedures (see 16.1.5); (ISO/IEC, 2013) section 12.6.1
		(ISO/IEC, 2013)	12.6.1	Define a procedure to address the situation where a vulnerability has been identified but there is no suitable countermeasure. In this situation, the organization should evaluate risks relating to the known vulnerability and define appropriate detective and corrective actions. (ISO/IEC, 2013) section 12.6.1
		(Souppaya & Scarfone, 2013)	3.1	Organizations should carefully consider the relevant issues related to timing, prioritization, and testing when planning and executing their enterprise patch management processes. (Souppaya & Scarfone, 2013)
		(Souppaya & Scarfone, 2022)	2.2.3.a	Prepare the risk response. This encompasses any preparatory activities, such as acquiring, validating, and testing patches for the vulnerable software; deploying additional security controls to safeguard the vulnerable software; or acquiring a replacement for a legacy asset that cannot be patched. It might also include scheduling the risk response and coordinating deployment plans with enterprise change management, business units, and others. (Souppaya & Scarfone, 2022)
		(ISO/IEC, 2022)	8.8	To evaluate identified technical vulnerabilities, the following guidance should be considered: analyse and verify reports to determine what response and remediation activity is needed;
		(ISO/IEC, 2022)	8.8	The following guidance should be considered to address technical vulnerabilities: depending on how urgently a technical vulnerability needs to be addressed, carrying out the action according to the controls related to change management (see 8.32) or by following information security incident response procedures (see 5.26);
	Business Requirements	(ISO/IEC, 2013)	12.5.1	Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release, e.g. the introduction of new information security functionality or the number and severity of information security problems affecting this version. Software patches should be applied when they can help to remove or reduce information security weaknesses (see 12.6). (ISO/IEC, 2013) section 12.5.1
		(Souppaya & Scarfone, 2013)	3.1	If a vulnerability is not being exploited yet, organizations should carefully weigh the security risks of not patching with the operational risks of patching without performing thorough testing first.
		IEC 2015	5	f) schedule authorized, effective patches for installation at the next available opportunity within the constraints of system design (for example, redundancy, fault-tolerance, safety) and operational requirements (for example, unplanned outage, scheduled outage, onprocess, etc.);

Continued on next page

Table 7 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
Standards	Scanning Tools	(ISO/IEC, 2022)	8.8	To identify technical vulnerabilities, the organization should consider: using vulnerability scanning tools suitable for the technologies in use to identify vulnerabilities and to verify whether the patching of vulnerabilities was successful;
		(ISO/IEC, 2022)	8.8	A weakness with vulnerability scanning is that it is possible it does not fully account for defence in depth: two countermeasures that are always invoked in sequence can have vulnerabilities that are masked by strengths in the other. The composite countermeasure is not vulnerable, whereas a vulnerability scanner can report that both components are vulnerable. The organization should therefore take care in reviewing and acting on vulnerability reports.
	Remediation	(ISO/IEC, 2022)	8.8	The following guidance should be considered to address technical vulnerabilities: develop remediation
	Source	(Souppaya & Scarfone, 2022)	2.3.1	Validate the patch. A patch's authenticity and integrity should be confirmed, preferably by automated means, before the patch is tested or installed. The patch could have been acquired from a rogue source or tampered with in transit or after acquisition.
		(ISO/IEC, 2022)	8.8	The following guidance should be considered to address technical vulnerabilities: only using updates from legitimate sources
Control Framework	Automation	(Center for Internet Security, n.d.-a)	Control 7; Safeguard 7.5	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
			Control 7; Safeguard 7.6	Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
	Vulnerability Assessment		Control 16; Safeguard 16.3	Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.
	Risk Assessment; Prioritisation		Control 16; Safeguard 16.6	Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.

E.3. Patch Testing

Table 8: Mapping for Patch Testing

Type	Aspect	Publication	Section	Guideline / Requirement
Regulations	Effectiveness	(European Parliament, 2022)	21.2	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 (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
	Test Environment	BIO	12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. Proceseigenaar Dienstenleverancier
		BIO	12.1.4.1	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken. 12.1.4.2 2 Wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.
		BIO	12.1.4.2	Wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.
	Test	(European Banking Authority et al., 2022)	10.4.c	test and deploy the software and hardware patches and the updates referred to in Article 8(2), point (b), points (v), (vi) and (vii);
Standards	Test	(Mell et al., 2005)	-	Conduct the testing of patches and non-patch remediation methods on IT devices that use standardized configurations.
		Souppaya 2002	2.3.1	Test the patch. A patch may be tested before deployment. This is intended to reduce operational risk by identifying problems with a patch before placing it into production. Testing may be performed manually or through automated methods.
		(ISO/IEC, 2022)	8.19	The following guidelines should be considered to securely manage changes and installation of software on operational systems: only installing and updating software after extensive and successful testing (see 8.29 and 8.31);
	Test Environment	(ISO/IEC, 2013)	12.5.1	Applications and operating system software should only be implemented after extensive and successful testing; the tests should cover usability, security, effects on other systems and userfriendliness and should be carried out on separate systems (see 12.1.4); it should be ensured that all corresponding program source libraries have been updated
		IEC 2013	5	e) test the installation of IACS patches in a way that accurately reflects the production environment, so as to ensure that the reliability and operability of the IACS is not negatively affected when patches are installed on the IACS in the actual production environment. Patches which have successfully passed these tests are called the 'authorized patches';
		(ISO/IEC, 2022)	8.31	In all cases, development and testing environments should be protected considering: patching and updating of all the development, integration and testing tools (including builders, integrators, compilers, configuration systems and libraries);
		(ISO/IEC, 2022)	8.32	Changing software can impact the production environment and vice versa. Good practice includes the testing of ICT components in an environment segregated from both the production and development environments (see 8.31). This provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes. This should include patches, service packs and other updates.
	Side Effects	(ISO/IEC, 2013)	12.6.1	Patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as: 1) turning off services or capabilities related to the vulnerability; 2) adapting or adding access controls, e.g. firewalls, at network borders (see 13.1); 3) increased monitoring to detect actual attacks; 4) raising awareness of the vulnerability;

Continued on next page

Table 8 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
		(ISO/IEC, 2013)	12.6.1	Vendors are often under significant pressure to release patches as soon as possible. Therefore, there is a possibility that a patch does not address the problem adequately and has negative side effects. Also, in some cases, uninstalling a patch cannot be easily achieved once the patch has been applied.
		(Souppaya & Scarfone, 2013)	3.4.3	Organizations should be capable of detecting side effects, such as changes to security configuration settings, caused by patch installation.
		(ISO/IEC, 2022)	8.8	The following guidance should be considered to address technical vulnerabilities: testing and evaluating updates before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated [i.e. if an update is available, assessing the risks associated with installing the update (the risks posed by the vulnerability should be compared with the risk of installing the update)];
Standards	Resource Constraints	(ISO/IEC, 2013)	12.6.1	If adequate testing of the patches is not possible, e.g. because of costs or lack of resources, a delay in patching can be considered to evaluate the associated risks, based on the experience reported by other users. The use of ISO/IEC 27031[14] can be beneficial.
		(ISO/IEC, 2022)	8.8	If adequate testing of the updates is not possible (e.g. because of costs or lack of resources) a delay in updating can be considered to evaluate the associated risks, based on the experience reported by other users. The use of ISO/IEC 27031 can be beneficial.
	Organisational Policy	(Mell & Tracy, 2002)	-	The patching policy should also include a methodology for testing and safely installing patches.
	Conflicts	(Souppaya & Scarfone, 2013)	3.2	Organizations should identify all the ways in which patches could be applied and act to resolve any conflicts among patch application methods.
	Authenticity	(ISO/IEC, 2022)	8.8	The following guidance should be considered to address technical vulnerabilities: provide mechanisms to verify the authenticity of remediation;
Control Framework	Test Environment	(Center for Internet Security, n.d.-a)	Control 16; Safeguard 16.8	Maintain separate environments for production and non-production systems.
	Test	(Center for Internet Security, n.d.-a)	Control 16; Safeguard 16.2	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.

E.4. Patch Deployment

Table 9: Mapping for Patch Deployment

Type	Aspect	Publication	Section	Guideline / Requirement
Regulations	Deploy	(European Banking Authority et al., 2022)	10.2.f	prioritise the deployment of patches and other mitigation measures to address the vulnerabilities identified;
		(European Banking Authority et al., 2022)	10.4.c	test and deploy the software and hardware patches and the updates referred to in Article 8(2), point (b), points (v), (vi) and (vii);
		(European Parliament, 2022)	21.e	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:(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
		(Dutch Central Government, 2018)	12.6	For software services within technical infrastructures, it should be verified whether the latest updates have been deployed, preferably through automation. Patches are not deployed automatically unless specific arrangements have been made with the software vendor.
Standards	Access Control	(ISO/IEC, 2013)	12.5.1	The updating of the operational software, applications and program libraries should only be performed by trained administrators upon appropriate management authorization (see 9.4.5)
		(Souppaya & Scarfone, 2013)	3.2	Organizations should ensure that users cannot disable or otherwise negatively affect enterprise patch management technologies, and organizations should perform continuous monitoring of enterprise patch management technologies to identify any issues that occur
		(Souppaya & Scarfone, 2022)	2.3.2	Distribute the patch. Distributing the patch to the assets that need to have it installed can be organization-controlled (and occur automatically, manually, or as scheduled) or vendorcontrolled, such as delivered from the cloud. (Souppaya & Scarfone, 2022)
	Policy	(Mell & Tracy, 2002)	-	The patching policy should also include a methodology for testing and safely installing patches.
	Scheduling	(Souppaya & Scarfone, 2022)	3.5.1	Organizations should consider adopting phased deployments for routine patching in which a small subset of the assets to be patched receive the patch first. These assets act as canaries (i.e., bellwethers) for identifying issues and determining the likely operational impact of the patch. In effect, this is how the patching gets tested. If the canary assets indicate that the patch should have minimal impact, the deployment can expand to more or all of the vulnerable assets. Significant problems can be addressed before the rollout expands, or a different risk response - like a temporary mitigation – can be planned instead of the patch while the problems are resolved.
	Configurations	(Souppaya & Scarfone, 2022)	2.3.2	Change software configuration and state. In some cases, making a patch take effect necessitates implementing changes. Examples include restarting patched software, rebooting the operating system or platform on which the patched software runs, redeploying the applications, or altering software configuration settings. In other cases, no such changes are needed. (Souppaya & Scarfone, 2022)
	Deployment Factors	(Souppaya & Scarfone, 2022)	2.3.2	Patch deployment varies widely based on several factors, including: • The type of software being updated (e.g., firmware, operating system [OS], application) • The asset platform type (e.g., IT, OT, IoT, mobile, cloud, virtual machine [VM], containers) • Platform traits, such as managed/unmanaged asset, on-premises or not, virtualized or not, and containerized or not • Environmental limitations, such as network connectivity and bandwidth
	Automation	(Mell et al., 2005)	-	Perform automated deployment of patches to IT devices using enterprise patch management tools. Configure automatic updates of applications whenever possible and appropriate.

Continued on next page

Table 9 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
Standards	Vendor	(ISO/IEC, 2022)	8.8	Where the vendor provides an automated update process and the updates can be installed on affected systems or products without the need for intervention, the organization determines if it applies the automated process or not. One reason for not electing for automated update is to retain control over when the update is performed. For example, a software used for a business operation cannot be updated until the operation has completed.
	Logging	(Mell et al., 2005)	-	Create a database of remediation methods that need to be applied within the organization. Oversee the vulnerability remediation process in the organization.
		(ISO/IEC, 2013)	12.5.1	An audit log should be maintained of all updates to operational program libraries;
		(ISO/IEC, 2013)	12.6.1	an audit log should be kept for all procedures undertaken;
Control Framework	Deploy; Automation; Timeline	(Center for Internet Security, n.d.-a)	Control 16; Safeguard 16.8	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
		(Center for Internet Security, n.d.-a)	Control 16; Safeguard 16.2	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

E.5. Post-Deployment Patch Verification

Table 10: Mapping for Post-Deployment Patch Verification

Type	Aspect	Publication	Section	Guideline / Requirement
Regulations	Monitor & Verify	(European Banking Authority et al., 2022)	10.2.g	monitor and verify the remediation of vulnerabilities
		(European Parliament, 2022)	21.e	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:e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
	Document	(European Banking Authority et al., 2022)	10.2.h	require the recording of any detected vulnerabilities affecting ICT systems and the monitoring of their resolution.
Standards	Verify	(Mell et al., 2005)	-	Measure the effectiveness of the patch and vulnerability management program in a consistent manner and apply corrective actions as necessary.
		(Mell et al., 2005)	-	Verify vulnerability remediation through network and host vulnerability scanning
		(Souppaya & Scarfone, 2013)	3.4.4	One option is to attempt to exploit the vulnerability, but this is generally only feasible if an exploit already exists, and there are substantial risks with attempting exploitation, even under highly controlled conditions. Organizations should use other methods of confirming installation, such as a vulnerability scanner that is independent from the patch management system.
		(Souppaya & Scarfone, 2022)	2.2.3.d	Verify the risk response. This step involves ensuring that the implementation has been completed successfully. For patching, this means confirming that the patch is installed and has taken effect. For deploying additional security controls, ensure they are functioning as intended. For risk avoidance, verify that vulnerable assets were decommissioned or replaced.
		(ISO/IEC, 2022)	8.8	To identify technical vulnerabilities, the organization should consider: using vulnerability scanning tools suitable for the technologies in use to identify vulnerabilities and to verify whether the patching of vulnerabilities was successful;
	Monitor	(ISO/IEC, 2013)	12.6.1	The technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency;
		(Souppaya & Scarfone, 2022)	2.3.4	Continuously monitor the risk response. Make sure that the risk response continues to be in place: no one uninstalls the patch, deactivates the additional security controls, lets the cybersecurity insurance lapse, or restarts the decommissioned asset.
		(Souppaya & Scarfone, 2022)	2.3.4	In the last phase of the life cycle, the patch's deployment can be monitored using automation to confirm that the patch is still installed. For example, monitoring could confirm that the patch has not been uninstalled by a user or an attacker, an unpatched version of the software has not been restored from a backup, and the device has not been reset to a vulnerable factory-default state.
		(Souppaya & Scarfone, 2022)	2.3.4	Another reason for monitoring the deployed patches is to see if the patched software's behavior changes after patching. As part of a layered security approach to mitigating supply chain risk, this might be helpful at detecting, responding to, and recovering from situations where the installed patch was itself compromised.
	Backup	(ISO/IEC, 2013)	12.5.1	Previous versions of application software should be retained as a contingency measure;
		(ISO/IEC, 2013)	12.5.1	Old versions of software should be archived, together with all required information and parameters
		(ISO/IEC, 2022)	8.19	The following guidelines should be considered to securely manage changes and installation of software on operational systems: defining a rollback strategy before changes are implemented;
		(ISO/IEC, 2022)	8.19	The following guidelines should be considered to securely manage changes and installation of software on operational systems: archiving old versions of software, together with all required information and parameters, procedures, configuration details and supporting software as a contingency measure, and for as long as the software is required to read or process archived data.

Continued on next page

Table 10 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
	Logging	IEC 2015	5	g) update records at a planned interval, at least on a quarterly basis, to include for each updateable device: installed versions, authorized versions, effective versions and released versions;
		(ISO/IEC, 2022)	8.19	The following guidelines should be considered to securely manage changes and installation of software on operational systems: maintaining an audit log of all updates to operational software;
	Side Effects	(Souppaya & Scarfone, 2022)	2.3.2	Resolve any issues. Installing a patch may cause side effects to occur, like inadvertently altering existing security configuration settings or adding new settings, and these side effects can inadvertently create a new security problem while fixing the original one. Patch installation can also cause operational issues that may necessitate uninstalling the patch, reverting to the previous version of the software, or restoring the software or asset from backups.
Control Framework	Verify & Monitor	(Center for Internet Security, n.d.-a)	Control 16; Safeguard 16.2	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.

E.6. Overall Process

Table 11: Mapping for Overall Process

Type	Aspect	Publication	Section	Guideline / Requirement
Regulations	Asset Inventory	BIO	8.1.1	Inventorying of assets: Information, other assets related to information, and information processing facilities must be identified, and an inventory of these assets must be created and maintained.
		BIO	8.1.2	Ownership of assets: Assets listed in the inventory should have an assigned owner.
	Proportionality	BIO	12.6.1	Management of Technical Vulnerabilities: Information about technical vulnerabilities in the information systems being used should be obtained in a timely manner, the organization's exposure to such vulnerabilities should be assessed, and appropriate measures should be taken to address the associated risk. BIO
		(European Parliament, 2022)	21.1	Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational 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. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.
		(European Banking Authority et al., 2022)	10.4.d	set deadlines for the installation of software and hardware patches and updates and escalation procedures in case those deadlines cannot be met.
	Liability	(European Parliament, 2022)	20.1	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. The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.
	Policy & Procedure	(European Parliament, 2022)	21.2	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: (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure; (g) basic cyber hygiene practices and cybersecurity training;
		(National Cyber Security Centre, 2023b)	6	Write Policy on the Security of Network and Information Systems: policy on security when acquiring, developing, and maintaining network and information systems, including response to and disclosure of vulnerabilities. Many companies and organizations rely on network and information systems for their core business processes. If access to these systems is lost or if information is exposed, it can have significant consequences for the organization.
		(National Cyber Security Centre, 2023b)	6	Write policy on Change Management Change management describes how an organization handles the implementation and monitoring of changes, repairs, and maintenance. A consistent procedure is crucial. The change management process should include at least the following: - Request for the change; - Possible risks and impact of the change; - Criteria for prioritizing changes and testing requirements; - Roll-back requirements (reversing changes); - Logging of changes

Continued on next page

Table 11 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
		(National Cyber Security Centre, 2023b)	6	Patch Management: To minimize vulnerabilities, it is important to install security updates (patches) as soon as possible. This is a basic principle of secure digital operations. Security updates improve software and close security gaps, enhancing digital resilience. The patch management policy should describe under what conditions security updates will be installed. Which systems are updated immediately, and which can wait? Test patches in a test environment before installation and check them for integrity and reliability. Follow the change management process when implementing patches.Note: Hardware and software products in your network may be End-of-Life (EoL), meaning they no longer receive patches. Ensure there is a policy for handling EoL products.
		(European Banking Authority et al., 2022)	10.1	As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement vulnerability management procedures.
		(European Banking Authority et al., 2022)	10.3	As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document and implement patch management procedures.
		(Dutch Central Government, 2018)	12.6	A process is established to manage technical vulnerabilities, which includes regular penetration testing, vulnerability risk analysis, and patch management.
		BIO	5.1.1.1	Beleidsregels voor informatiebeveiliging Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
	Critical & Important Functions	(European Banking Authority et al., 2022)	8.1	As part of the ICT risk management framework referred to in Article 6(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation.
	Asset Inventory	(European Banking Authority et al., 2022)	8.4	Financial entities shall identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment, and shall map those considered critical. They shall map the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets.
		(European Banking Authority et al., 2022)	8.6	For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories and update them periodically and every time any major change as referred to in paragraph 3 occurs.
	Third-Party	(European Banking Authority et al., 2022)	8.5	Financial entities shall identify and document all processes that are dependent on ICT third-party service providers, and shall identify interconnections with ICT third-party service providers that provide services that support critical or important functions.
		(European Banking Authority et al., 2022)	10.2.c	verify whether: (i) ICT third-party service providers handle vulnerabilities related to the ICT services provided to the financial entity; (ii) whether those service providers report to the financial entity at least the critical vulnerabilities and statistics and trends in a timely manner; For the purposes of point (c), financial entities shall request that ICT third-party service providers investigate the relevant vulnerabilities, determine the root causes, and implement appropriate mitigating action.
		(European Banking Authority et al., 2022)	10.2.d	track the usage of: (i) third-party libraries, including open-source libraries, used by ICT services supporting critical or important functions; (ii) ICT services developed by the financial entity itself or specifically customised or developed for the financial entity by an ICT third-party service provider; For the purposes of point (d), financial entities shall, where appropriate in collaboration with the ICT third-party service provider, monitor the version and possible updates of the third-party libraries. In case of ready to use (off-the-shelf) ICT assets or components of ICT assets acquired and used in the operation of ICT services not supporting critical or important functions, financial entities shall track the usage to the extent possible of third-party libraries, including open-source libraries.
		BIO	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie: Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.

Continued on next page

Table 11 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
Regulations	Automation	(European Banking Authority et al., 2022)	10.4.a	The patch management procedures referred to in paragraph 3 shall: to the extent possible identify and evaluate available software and hardware patches and updates using automated tools;
	Emergency & Escalation	(European Banking Authority et al., 2022)	10.4.b	The patch management procedures referred to in paragraph 3 shall: identify emergency procedures for the patching and updating of ICT assets;
	Timeline	BIO	12.6	Patches for vulnerabilities with a high likelihood of exploitation and significant potential impact should be deployed as quickly as possible, ideally within one week. Less critical patches should be scheduled for the next available maintenance window.
		(Dutch Central Government, 2018)	12.6.2.1	If the likelihood of exploitation and the expected damage are both high (NCSC classification of vulnerability warnings), patches are installed as soon as possible, but no later than within a week. In the meantime, mitigating measures are taken based on an explicit risk assessment.
	Access Control	BIO	12.6.1	Restrictions on software installation: Rules should be established and implemented for users installing software updates.
		BIO	12.6.2.1	Users cannot install anything on their work environment themselves, except for what is provided or permitted by the ICT provider (whitelist).
	Policy & Procedure	(Mell & Tracy, 2002)	-	Organizations should have an explicit and documented patching and vulnerability policy as well as a systematic, accountable, and documented set of processes and procedures for handling patches.
		(Mell & Tracy, 2002)	-	The patching and vulnerability policy should specify what techniques an organization will use to monitor for new patches and vulnerabilities and which personnel will be responsible for such monitoring.
		(Souppaya & Scarfone, 2013)	5	Organizations should implement and use appropriate measures for their enterprise patch management technologies and processes.
		(Souppaya & Scarfone, 2013)	3.3	Organizations should carefully consider all alternative host architectures in use for the enterprise when designing enterprise patch management policies and solutions
		IEC 2015	4.4	Patches have a defined lifecycle state model. They progress from available to authorized to effective and installed. Not all patches available are relevant to the IACS and not all patches are compatible with the IACS applications. It is important for an effective IACS patch management process to know the state of all available patches.
		(Souppaya & Scarfone, 2022)	2.2	In addition, there are administrative activities occurring throughout the software vulnerability management life cycle, such as updating documentation, audit logging, and generating actionable insights and reports as part of enterprise change management. Having robust change management policies and processes in place is a fundamental part of software vulnerability management.
		(Souppaya & Scarfone, 2022)	8.8	The organization should develop procedures and capabilities to: b) receive vulnerability reports from internal or external sources.
		(ISO/IEC, 2022)	8.8	The organization should develop procedures and capabilities to: a) detect the existence of vulnerabilities in its products and services including any external component used in these;
		(ISO/IEC, 2022)	8.8	An effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out in case an incident occurs.
	Asset Inventory	(Mell et al., 2005)	-	Inventory the organization's IT resources to identify the hardware equipment, operating systems, and software applications that are used within the organization.
		(ISO/IEC, 2013)	12.6.1	A current and complete inventory of assets (see Clause 8) is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organization responsible for the software.
		(ISO/IEC, 2013)	12.6.1	Asset Inventory Management is another essential prerequisite for patch and vulnerability management.

Continued on next page

Table 11 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
		IEC 2015	5	IACS asset owners should: a) establish and maintain an inventory of all electronic devices associated with the IACS, that may be updated by: modification of their functionality, configuration, operation, software, firmware, operating code, etc. These devices should be referred to as 'updatable' devices;
		IEC 2015	5	b) establish and maintain an accurate record of the currently installed versions for each device, called the 'installed' version;
		(Souppaya & Scarfone, 2022)	3.2	Organizations should approach patching from a per-asset perspective. Software inventories should include information on each computing asset's technical characteristics and mission/business characteristics. Making decisions for risk responses and their prioritization should not be based solely on which software and software versions are in use. Each asset has technical and mission/business characteristics that should be taken into consideration because they provide context for the vulnerable software running on that asset.
		(Souppaya & Scarfone, 2022)	3.2	The characteristics that an organization should inventory will vary, but the following are examples of possible characteristics to track: • The asset's platform type (e.g., IT, OT, IoT, mobile, cloud, VM) • The party who administrates the asset (e.g., IT department, third party, end user, vendor/manufacturer, shared responsibility model) • The applications, services, or other mechanisms used to manage the asset (e.g., endpoint management software, virtual machine manager, container management software) • The asset's network connectivity in terms of protocols, frequency/duration, and bandwidth • The technical security controls already in place to safeguard the asset • The asset's primary user(s) or interconnected services and their privileges
		(Souppaya & Scarfone, 2022)	3.2	Examples of mission/business characteristics that an organization should track include: • The asset's role and importance to the organization, which are contextual and may be hard to define or determine (Souppaya & Scarfone, 2022) 89 • Laws, regulations, or policies that specify how soon a new vulnerability in the asset must be addressed • Contractual restrictions on patching (e.g., a highly regulated asset can only be patched by its manufacturer after testing and certification) • Mission/business restrictions on risk responses for that asset (e.g., an asset can only be rebooted during a monthly maintenance outage)
		(Souppaya & Scarfone, 2022)	3.2	Organizations should establish and constantly maintain up-to-date software inventories for their physical and virtual computing assets, including OT, IoT, and container assets. This information could be in a single enterprise asset inventory, or it could be split among multiple resources. While a comprehensive inventory of all assets is ideal, it may be impossible to achieve, given the highly dynamic nature of assets and software. A realistic goal is to maintain a close-to-comprehensive inventory by relying on automation to constantly discover new assets and collect up-to-date information on all assets.
		(Souppaya & Scarfone, 2022)	3.2	Without constant updates, inventories will quickly become outdated and provide increasingly inaccurate and incomplete information for patching efforts. At one time, when assets and software were mostly static and were located within static logical and physical perimeters, it was generally considered acceptable to update inventories on a monthly or quarterly basis by performing a vulnerability scan. That model should no longer be used.
		(Souppaya & Scarfone, 2022)	3.2	Constantly updating inventories for all of the technologies and environments in use today requires a combination of automation techniques and tools. Organizations should leverage inventory capabilities built into platforms and assets whenever feasible. For example, APIs built into a cloud-based platform may enable continuous updates of inventory information for the software on that platform, as well as other platform characteristics helpful for patch management purposes. Vulnerability scans and passive network monitoring on local networks can still contribute to asset inventories, especially in terms of asset discovery. If vulnerability scans are to be used for software inventories, they will need sufficient access to the assets (i.e., authenticated scanning) in order to detect changes to their software and other technical characteristics.
		(Souppaya & Scarfone, 2022)	2.2	Know when new software vulnerabilities affect your organization's assets, including applications, operating systems, and firmware.
		(ISO/IEC, 2022)	8.8	The organization should have an accurate inventory of assets (see 5.9 to 5.14) as a prerequisite for effective technical vulnerability management; the inventory should include the software vendor, software name, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organization responsible for the software.

Continued on next page

Table 11 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
	Roles & Responsibilities	(ISO/IEC, 2013)	12.6.1	Roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required should be defined and established
		(Souppaya & Scarfone, 2022)	3.4	Organizations should use the software inventories, technical and business/mission characteristics, and risk response scenarios to assign each asset to a maintenance group. A maintenance group is a set of assets with similar characteristics that generally have the same software maintenance needs for each risk response scenario. Maintenance needs include not only patching (e.g., patch schedule, patch testing needs, outage restrictions, level of impact if vulnerable software is compromised) but also any other appropriate forms of mitigation and risk response, such as temporary mitigations used when patches are not yet available.
		(Souppaya & Scarfone, 2022)	3.4	Organizations should define their maintenance groups at whatever they decide the best level of granularity is, then periodically reassess their maintenance group definitions and adjust them as needed. Here are a few simplified examples of possible maintenance groups: • Mobile workforce laptops for standard end users • On-premises datacenter (including servers, network equipment, storage, etc.) • Legacy OT assets • Smartphones for the mobile workforce • On-premises servers for automated software testing • Containers with customer-facing applications in the public cloud Maintenance groups can also be defined based on other characteristics, like personnel roles (e.g., software developer workstations, system administrator workstations) or asset importance (e.g., low-impact IoT consumer assets, OT and IoT assets with lifesafety impact).
	Configuration Control	(ISO/IEC, 2013)	12.6.1	A configuration control system should be used to keep control of all implemented software as well as the system documentation.
	Third-Party	(ISO/IEC, 2013)	12.5.1	Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organization should consider the risks of relying on unsupported software.
		(ISO/IEC, 2013)	12.5.1	Physical or logical access should only be given to suppliers for support purposes when necessary and with management approval. The supplier's activities should be monitored.
		(ISO/IEC, 2013)	12.5.1	Computer software may rely on externally supplied software and modules, which should be monitored and controlled to avoid unauthorized changes, which could introduce security weaknesses.
		(Souppaya & Scarfone, 2022)	3.1	Possible methods for decreasing the number of vulnerabilities include: • Acquire software that is likely to have fewer vulnerabilities over time compared to other software.
		(Souppaya & Scarfone, 2022)	3.1	Possible methods for decreasing the number of vulnerabilities include: • Work with software development partners that are likely to introduce fewer vulnerabilities into software over time, taking into consideration factors such as how rigorous their secure software development practices are, how quickly they address issues and release patches, how often problems are associated with their patches, and how transparent they are in their security-related communications.
		(Souppaya & Scarfone, 2022)	3.1	Possible methods for decreasing the number of vulnerabilities include: • Use managed services instead of software when feasible.
		(Souppaya & Scarfone, 2022)	3.7	Organizations should take software maintenance into consideration when procuring software. Software maintenance is one factor of many that organizations should consider.
		(ISO/IEC, 2022)	8.8	tracking the usage of third-party libraries and source code for vulnerabilities. This should be included in secure coding (see 8.28).

Continued on next page

Table 11 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
		(ISO/IEC, 2022)	8.8	Where the organization uses a cloud service supplied by a third-party cloud service provider, technical vulnerability management of cloud service provider resources should be ensured by the cloud service provider. The cloud service provider's responsibilities for technical vulnerability management should be part of the cloud service agreement and this should include processes for reporting the cloud service provider's actions relating to technical vulnerabilities (see 5.23). For some cloud services, there are respective responsibilities for the cloud service provider and the cloud service customer. For example, the cloud service customer is responsible for vulnerability management of its own assets used for the cloud services.
	Business Requirements	(Souppaya & Scarfone, 2013)	4.3.3	Organizations should balance their security needs with their needs for usability and availability.
	Principles	(Souppaya & Scarfone, 2022)	3	Recommendations support the following principles, which organizations should strive to adopt in their enterprise patch management practices: • Problems are inevitable; be prepared for them. Risk responses, including patching, will never be perfect. Some may inadvertently cause operational problems, for example, but most will not. To improve enterprise patch management, organizations need to change their culture so that instead of fearing problems and thus delaying risk responses, personnel are prepared to address problems when they occur. The organization needs to become more resilient, and everyone in the organization needs to understand that problems caused by patching are a necessary inconvenience that helps prevent major compromises.
		(Souppaya & Scarfone, 2022)	3	Recommendations support the following principles, which organizations should strive to adopt in their enterprise patch management practices: • Simplify decision making. Conducting a risk assessment of each new vulnerability in order to plan the optimal risk response for it is simply not feasible. Organizations do not have the time, resources, expertise, or tools to do so. Planning needs to be done in advance so that when a new vulnerability becomes known, a decision can quickly be made about how to respond to it.
		(Souppaya & Scarfone, 2022)	3	Recommendations support the following principles, which organizations should strive to adopt in their enterprise patch management practices: • Rely on automation. There is no way that an organization can keep up with patching without automation because of the sheer number of assets, software installations, vulnerabilities, and patches. Automation is also needed for emergency situations, like patching a severe vulnerability that attackers are actively exploiting. Having automation in place gives an organization agility and scalability when it comes to its risk responses.
		(Souppaya & Scarfone, 2022)	3	Recommendations support the following principles, which organizations should strive to adopt in their enterprise patch management practices: • Start improvements now. Some of the changes that an organization may need to make might take years to put in place, but that does not mean that other practices cannot be improved in the meantime.
		(Souppaya & Scarfone, 2022)	3.1	Organizations should strive to decrease the number of vulnerabilities introduced into their environments. This shrinks the attack surface and can lower the amount of patching that organizations need to do. Possible methods for decreasing the number of vulnerabilities include: • Harden software, such as enforcing the principles of least privilege and least functionality (e.g., deactivating or uninstalling software services, features, and other components that are not needed).
	Architecture & System Considerations	(Souppaya & Scarfone, 2022)	3.1	Possible methods for decreasing the number of vulnerabilities include: • Select stacks or platforms that are likely to have fewer vulnerabilities over time compared to other stacks or platforms (e.g., running software within a small container instead of a larger operating system).
		(Souppaya & Scarfone, 2022)	3.1	Organizations should consider deploying applications in ways that make patching less likely to disrupt operations. One example is to run applications on stacks or platforms where patching is a fundamental part of the deployed technology and is less likely to disrupt operations (e.g., modernizing and running software within cloud-based containers instead of on-premises server operating systems). Another example is to take advantage of existing toolchains that already build applications with updated components and test them before production release.

Continued on next page

Table 11 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
	Scenario Planning	(Souppaya & Scarfone, 2022)	3.5	Organizations should define a maintenance plan for each maintenance group for each applicable risk response scenario. A maintenance plan defines the actions to be taken when a scenario occurs for a maintenance group, including the timeframes for beginning and ending each action, along with any other pertinent information. Along with the maintenance plans, organizations should define a risk assessment process for determining which plan should be used at any given time and for deciding when to switch from one plan to another as the understanding of risk changes.
		(Souppaya & Scarfone, 2022)	3.3	Organizations should define the software vulnerability risk response scenarios they need to be prepared to handle. Examples of such scenarios include: • Routine patching. This is the standard procedure for patches that are on a regular release cycle and have not been elevated to emergency status. Most patching falls under this scenario. However, because routine patching does not have the urgency of emergency scenarios, and routine patch installation can interrupt operations (e.g., device reboots), it is often postponed and neglected. This provides many additional windows of opportunity for attackers. Delaying routine patching also makes emergency patching more difficult, time-consuming, and disruptive because of the need to first install previous patches that new patches depend upon. • Emergency patching. This is the procedure to address patching emergencies in a crisis situation, such as a severe vulnerability or a vulnerability being actively exploited. If one or more of the organization's vulnerable assets have already been compromised, emergency patching may be part of incident response efforts. Emergency patching needs to be handled as efficiently as possible to prevent the imminent exploitation of vulnerable assets. • Emergency mitigation. This is the emergency procedure in a crisis situation, like those described above for the emergency patching scenario, to temporarily mitigate vulnerabilities before a patch is available. The mitigation can vary and may or may not need to be rolled back afterward. Emergency mitigations are sometimes needed because of issues with a patch. For example, a patch might be flawed and not actually correct a vulnerability, or a patch might inadvertently disrupt the operation of other software or systems. A patch could even be compromised.
		(Souppaya & Scarfone, 2022)	3.3	• Unpatchable assets. This is the implementation of isolation or other methods to mitigate the risk of systems that cannot be easily patched. This is typically required if routine patching is not able to accommodate these systems within a reasonable time frame. Examples of why an asset may be unpatchable include the vendor not providing patches (e.g., asset is at end-of-life, asset does not support updates) or an asset needing to run uninterrupted for an extended period of time because it provides mission-critical functions. Unpatchable assets need to be included in risk response planning because a new vulnerability in an asset might necessitate a change in the methods needed to mitigate its risk.
		(Souppaya & Scarfone, 2022)	3.5.4	Organizations should plan to implement multiple types of mitigations to protect vulnerable unpatchable assets. In addition to using long-term risk mitigation methods for unpatchable assets, organizations should also implement mitigations as needed to prevent exploitation of specific vulnerabilities that the long-term risk mitigation methods don't adequately address.
		(Souppaya & Scarfone, 2022)	3.5.4	Organizations should plan on periodically reevaluating their alternatives to patching. There are two main aspects to this. One is conducting a risk assessment to see if the alternatives to patching are still sufficiently effective at mitigating risk. The other is conducting a cost-benefit analysis to see if the assets provide sufficient value to the organization compared with the additional costs of mitigating, transferring, or accepting the risk of unpatchable assets.
		(Souppaya & Scarfone, 2022)	3.5.5	Organizations should closely track and monitor all exceptions to maintenance plans. As explained in Section 3.4, maintenance groups should be defined to minimize assets considered "exceptions." However, having some exceptions is inevitable. All exceptions to maintenance plans should be reviewed regularly to determine if the maintenance plan can be implemented now. Assets with similar long-term exceptions might need to be moved to a separate maintenance group with its own maintenance plan.

Continued on next page

Table 11 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
	Inability to patch	(Souppaya & Scarfone, 2022)	3.5.4	Organizations should plan to implement multiple types of long-term risk mitigation methods besides patching to protect vulnerable assets. There should be an approved set of methods for each maintenance group, and these methods should have been reviewed and analyzed in advance by security architects/engineers to determine their adequacy in mitigating risk.
		(ISO/IEC, 2022)	8.8	i) if no update is available or the update cannot be installed, considering other controls, such as: 1) applying any workaround suggested by the software vendor or other relevant sources; 2) turning off services or capabilities related to the vulnerability; 3) adapting or adding access controls (e.g. firewalls) at network borders (see 8.20 to 8.22); 4) shielding vulnerable systems, devices or applications from attack through deployment of suitable traffic filters (sometimes called virtual patching); 5) increasing monitoring to detect actual attacks; 6) raising awareness of the vulnerability.
	Timeliness	(Souppaya & Scarfone, 2022)	3.5.1	Organizations should offer flexibility with how soon routine patches are to be installed, while also forcing installation after a grace period has ended. A routine patch does not necessitate immediate installation, but at some point, patches must be installed to reduce the risk for the entire environment. Forcing installation can be direct, like triggering patch execution, or indirect, like preventing network access for unpatched assets until they are patched.
	Emergency	(Souppaya & Scarfone, 2022)	3.5.1	The organization should develop procedures and capabilities to: b) receive vulnerability reports from internal or external sources.
		(Souppaya & Scarfone, 2022)	3.5.3	Organizations should plan for the quick implementation of multiple types of emergency mitigations to protect vulnerable assets. Mitigations may require deactivating system functionality or isolating an asset from other assets and having automated mechanisms to apply these changes. Without the processes, procedures, and tools in place to implement mitigations, too much time may be lost, and vulnerable assets may be compromised.
		(Souppaya & Scarfone, 2022)	3.5.3	Organizations should plan to replace emergency mitigations with permanent fixes. Once a permanent fix, such as a patch, is available, the patch will need to be deployed and the mitigation removed. Schedules should be set and enforced for both patch deployment and mitigation removal.
	Logging	(ISO/IEC, 2022)	8.8	An audit log should be kept for all steps undertaken in technical vulnerability management.
	Authorized personnel	(ISO/IEC, 2022)	8.19	The following guidelines should be considered to securely manage changes and installation of software on operational systems: a) performing updates of operational software only by trained administrators upon appropriate management authorization
Control Framework	Asset Inventory	(Center for Internet Security, n.d.-a)	Control 1; Safeguard 1.1	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.
		(Center for Internet Security, n.d.-a)	Control 2; Safeguard 2.2	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.
	Policy & Procedure	(Center for Internet Security, n.d.-a)	Control 7; Safeguard 7.1	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

Continued on next page

Table 11 – continued from previous page

Type	Aspect	Publication	Section	Guideline / Requirement
		(Center for Internet Security, n.d.-a)	Control 7; Safeguard 7.2	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
	Automation; Timelines	(Center for Internet Security, n.d.-a)	Control 7; Safeguard 7.3	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
		(Center for Internet Security, n.d.-a)	Control 7; Safeguard 7.4	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
	Automation; Vulnerability Scanning	(Center for Internet Security, n.d.-a)	Control 7; Safeguard 7.5	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
		(Center for Internet Security, n.d.-a)	Control 7; Safeguard 7.6	Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
	Timelines	(Center for Internet Security, n.d.-a)	Control 7; Safeguard 7.7	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.