

Effects of the Cyber Resilience Act (CRA) on Industrial Equipment Manufacturing Companies

Roosa Risto^[0009-0005-3138-913X],
Mohit Sethi^[0000-0002-9730-1955], and
Mika Katara^[0009-0003-5512-9442]

KONE Corporation
firstname.lastname@kone.com

Abstract. The Cyber Resilience Act (CRA) is a new European Union (EU) regulation aimed at enhancing the security of digital products and services by ensuring they meet stringent cybersecurity requirements. This paper investigates the challenges that industrial equipment manufacturing companies anticipate while preparing for compliance with CRA through a comprehensive survey. Key findings highlight significant hurdles such as implementing secure development lifecycle practices, managing vulnerability notifications within strict timelines, and addressing gaps in cybersecurity expertise. This study provides insights into these specific challenges and offers targeted recommendations on key focus areas, such as tooling improvements, to aid industrial equipment manufacturers in their preparation for CRA compliance.

Keywords: CRA, Regulation, Challenges, Survey, IEC-62443, Standards

1 Introduction

The EU Cyber Resilience Act (CRA) [8] sets common security requirements for all products with digital elements within the EU. This broad scope intentionally covers all software and hardware products, as well as their remote data processing solutions, with exceptions for medical devices, aeronautical equipment, etc. which are already subject to similar existing EU regulations. The primary goal of the CRA is to enhance cybersecurity across the European Union by ensuring that products with digital elements are designed, developed, and maintained with robust security measures. While the act imposes requirements on many stakeholders, a significant portion of these requirements are directed towards manufacturers. The requirements for manufacturers can broadly be classified into software development lifecycle (SDL) process requirements, technical requirements, vulnerability management and notification requirements, and preparation of technical and user documentation.

The **SDL and technical** requirements outlined in Annex I Part I of the act require manufacturers to perform a risk assessment and subsequently ensure an appropriate level of cybersecurity throughout the design, development, and production process based on the risk assessment. SDL practices must ensure that

the products are free of known exploitable vulnerabilities, configured securely by default, and support timely security updates, including automatic updates with opt-out options. Additional technical measures include protecting data confidentiality, integrity, and availability through mechanisms like encryption and access controls, minimizing attack surfaces, implementing resilience against denial-of-service attacks, and data minimization. Furthermore, technical measures must also ensure logging of security-relevant activity, possibility of secure data removal, and mitigation of negative impact on other devices or networks.

Annex I Part II of the CRA sets forth **vulnerability management** requirements, obligating manufacturers to identify and document components and vulnerabilities in their products, including the creation of a software bill of materials (SBOM) in a standard, machine-readable format. Manufacturers are also required to address and remediate vulnerabilities promptly, providing security updates as necessary. When releasing a security update, the manufacturers must publicly disclose details about the fixed vulnerabilities, such as impacts, severity, and remediation steps. Lastly, manufacturers must perform regular testing to identify new vulnerabilities.

CRA specifies **vulnerability notification** practices in articles 14 and 15, mandating manufacturers to inform the European Union Agency for Cybersecurity (ENISA) and national computer security incident response teams (CSIRTs) within 24 hours of identifying actively exploited vulnerabilities or severe cyber incidents. The initial notification is followed by a detailed report within 72 hours, and a final report within 14 days for actively exploited vulnerabilities and within one month for other incidents. Manufacturers are also encouraged to voluntarily report near misses or incidents impacting the security of their products.

User documentation requirements listed in Annex II of CRA expect manufacturers to provide documentation containing, among other things, contact details for reporting vulnerabilities, the name and type information for uniquely identifying the product, information on the intended purpose of the product, detailed guidance on secure commissioning, update installation, and decommissioning, the type and duration of technical security support, and optionally, access to the product SBOM.

Requirements in Annex VII of CRA instruct that **technical documentation** must include a general description of the product, its intended purpose, relevant software versions, and, for hardware products, visual representations like photographs or diagrams of external and internal interfaces. Additionally, the technical documentation should detail the cybersecurity risk assessments performed, the SDL practices followed, the system architecture designed and developed, a list of applicable standards with which the product is compliant, as well as test reports verifying conformity with the technical requirements in those standards, and potentially the product SBOM.

Figure 1 shows the timeline for when different CRA requirements come into force. The final CRA text was published on 20 November 2024, implying that the transition period for vulnerability notification responsibilities will end on 11 September 2026, and all CRA requirements will become mandatory from 11

December 2027. Given the substantial requirements imposed on manufacturers

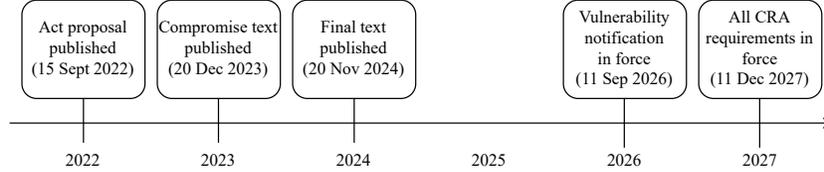


Fig. 1: CRA timeline

and the relatively short timeline for compliance, we conducted a quick survey to pinpoint the specific challenges faced by industrial equipment manufacturing companies. Our goal was to identify their pain points and offer targeted recommendations to aid in their preparation for compliance.

2 Previous Work on CRA Challenges

Szedlak et al. [15] examine the awareness and preparedness of SMEs for CRA. Their findings reveal significant disparities in CRA awareness and readiness, with only 12.3% of SMEs being aware of the CRA compared to 83.5% of very large enterprises.

Thiel [16] in his article discusses challenges in CRA compliance, particularly ensuring third-party components being integrated into products also meet CRA standards. He also highlights the issue of lacking in-house cybersecurity expertise, which may necessitate the need for external support.

The European Cyber Security Organisation (ECSO) conducted an online survey to identify potential challenges linked to the implementation of CRA [10]. The survey participants included a subset of ECSO members, primarily security service providers and manufacturers of digital devices, along with other public and private organizations. The survey revealed several key challenges, including the lack of clarity with product categories, the proposed timeline for implementation, and the need for clear guidelines on conducting risk and conformity assessments. Respondents emphasized the necessity for harmonized standards and methodologies at the EU level, as well as the importance of guidelines, templates, and training to facilitate CRA implementation.

A joint letter by experts published by the Center for Cybersecurity Policy and Law [9] raised concerns about the CRA's vulnerability disclosure requirements, including risks of misuse by governments, potential compromise of the vulnerability database by malicious actors, and discouraging effect on collaboration among manufacturers and researchers. The letter emphasizes the need for a risk-based approach, considering factors such as the severity of the vulnerability, the availability of mitigations, the potential impact on users, and the likelihood of broader exploitation.

A blog post by the Open Source Initiative [13] captures feedback on the draft text of CRA from various organizations in the open source community, highlighting concerns such as the unclear scope of exemptions for open source software, the risk of imposing disproportionate regulatory burdens on non-commercial contributors, and potential disruption to collaborative development models.

Schoo [14] in his paper examines some of the challenges from the Cyber Resilience Act (CRA). Among other things, he highlights the need for establishing uniform cybersecurity standards across the European Union and the necessity for a significant increase in the number of conformity assessment bodies to effectively manage and enforce these standards.

While previous work highlighted several challenges associated with CRA, our survey focuses on investigating the specific challenges that CRA poses for industrial equipment manufacturing companies. By identifying these challenges, we aim to provide a comprehensive understanding of how CRA impacts industrial equipment manufacturers and offer insights into effective strategies in key focus areas for seamless CRA compliance.

3 CRA and IEC 62443

CRA [8] in Annex VIII offers four conformity assessment options, including internal control, where manufacturers self-declare conformity, and EU-type examination, where a notified body verifies conformity before issuing a certificate. Harmonized standards play a pivotal role in all assessment options. As noted in recital 79 of the act, harmonized standards translating CRA’s requirements into detailed technical specifications, offer manufacturers clear and actionable compliance guidelines. Recital 81 further underscores that products with digital elements certified or declared in conformity with harmonized standards will benefit from a presumption of conformity, streamlining the compliance process.

The IEC 62443 series of standards provides a comprehensive framework for securing industrial automation and control systems (IACS) against cybersecurity threats. This series of standards is likely to form the basis for any harmonized standard used for CRA compliance by industrial equipment manufacturing companies. This is also evident from the ECSO survey on CRA challenges [10], which noted IEC 62443 as one of the most quoted standards by survey participants. While CENELEC, the European electrotechnical standards body, and specialized industrial equipment manufacturers may develop other harmonized standards, they will still reuse the IEC 62443 series as the building block. For example, the ISO 8102-20 [7] standard for elevators is based on IEC 62443.

The IEC 62443 standard series is structured into multiple parts, addressing different aspects of security, from general concepts and policies to technical requirements and processes. Among these, the parts relevant for CRA requirements include IEC 62443-4-1 [4], which outlines secure product development lifecycle (SDL) requirements for vendors; IEC 62443-4-2 [5], which specifies technical security requirements for IACS components, such as controllers and software applications; and IEC 62443-3-2 [6], which focuses on security risk assessment

and system design. The relevance of these standards for CRA compliance is also captured in the standard mapping report prepared by the European Union Agency for Cybersecurity (ENISA) [12].

In the survey, our questions to participants primarily focused on the IEC 62443-4-1 SDL process requirements necessary for CRA compliance, since following this process ensures that a suitable risk analysis is performed and that technical requirements, such as confidentiality and integrity protection of transmitted and stored data, are met. In addition to SDL process challenges, the survey included questions about the challenges of vulnerability notification and user instructions documentation requirements.

4 Study Design

Between June and August 2024, we conducted a survey to gather insights into the compliance challenges faced by industrial equipment manufacturing companies. The survey utilized an online questionnaire with 44 questions focused on CRA and IEC 62443-4-1 compliance. The questionnaire included both multiple-choice and freeform questions. Participants completed the questionnaire during one hour video meetings, where they could provide feedback using the think-aloud protocol. This approach helped capture comments that might otherwise have been missed, especially for the freeform qualitative questions. All meetings were hosted by the same author, and the survey questionnaire was shared with participants prior to the video meeting. Each session concluded with a discussion to gather broader feedback on challenges and potential solutions.

A total of 12 companies participated in the survey. This group included seven large companies (with over 500 employees) that manufacture industrial equipment such as cranes, elevators, and machinery for the shipping and mining industries. The remaining five companies were consultancies or partner organizations providing software and support services to the large industrial equipment manufacturers we surveyed. For each company, we ensured that the survey was answered by a senior technical cybersecurity manager who had a comprehensive understanding of both the organizational perspective and the technical challenges. Only one response per company was allowed, although multiple cybersecurity experts from the organization could join the calls. In fact, for two of the 12 companies, more than one expert participated in answering the questions. All participating companies had a sizable portion of their revenues in Europe, which motivated their interest in maintaining compliance in the region.

During the survey, we used the CRA text from December 2023 [11]. Participants were aware that the final text would be published in the first half of 2024, with a 21-month transition period for notification responsibilities ending in 2026, and a 36-month period for other responsibilities ending in 2027. Given that these expected timelines were similar to the final dates, it is unlikely that the survey responses were significantly affected.

Baseline Understanding Before delving into questions about compliance challenges, we wanted to gauge the familiarity of the participants with the IEC

62443-4-1 standard and the relatively new CRA regulation. As shown in Figure 2, most participants were familiar with both IEC 62443-4-1 and CRA, with 75% (9 out of 12) companies being quite or very familiar. Given that the IEC 62443 series of standards has been around for several years, it is not surprising that participants were more familiar with it compared to CRA. While participants demonstrated familiarity with both the standard and the regulation, they were allowed and encouraged to consult the official text during the survey and if any participant had questions about specific requirements, we provided assistance by referring to the relevant sections in the text.

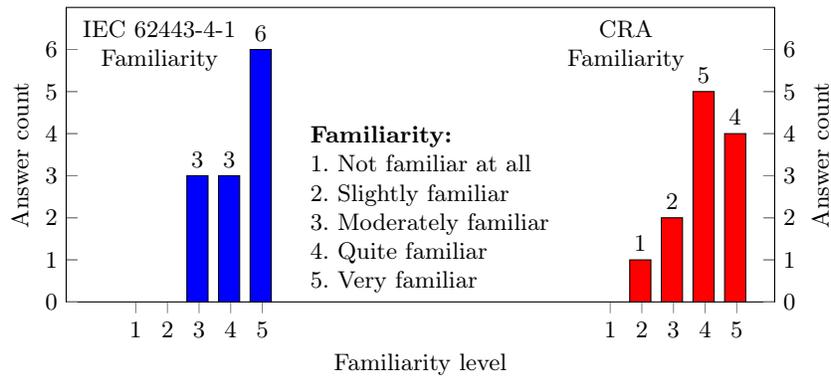


Fig. 2: Participant familiarity with IEC 62443-4-1 and CRA.

IEC 62443-4-1 includes different levels of maturity: Maturity Level 1 (Initial), Maturity Level 2 (Managed), Maturity Level 3 (Defined/Practiced), and Maturity Level 4 (Improving). All of the industrial equipment manufacturing companies interviewed had already established an internal SDL compliant with IEC 62443-4-1, and a few of them had reached Maturity Level 3, meaning they were actively practicing the SDL. Several manufacturers had even undergone third-party audits and obtained certifications. Naturally, the consulting and partner companies followed the SDL practices of the equipment manufacturing companies they worked with to ensure their customers remained compliant but were not developing their own SDL.

Limitations We recruited survey participants based on their involvement in a joint research project focused on automating compliance with the IEC 62443 series of standards. Additional participants were invited through recommendations from those already involved. All participating companies were predominantly based in Northern Europe, which may limit the generalizability of the findings to all industrial manufacturers subject to the CRA. Although some participants were international, with products sold outside the EU and not subject to CRA, the challenges faced by manufacturers outside the EU but selling products in the EU may differ. Another limitation is the small sample size of 12 compa-

nies, which makes it inappropriate to draw statistically significant conclusions. This limitation highlights the qualitative nature of our study, which is primarily descriptive and exploratory rather than statistically validated. Nonetheless, the findings provide valuable insights into the challenges faced by industrial equipment manufacturers. Since the focus was on identifying challenges specific to industrial equipment manufacturers, the recommendations may not apply to manufacturers of other products, such as consumer electronics.

5 Challenges

IEC 62443-4-1 organizes the SDL requirements into eight distinct practices, covering various aspects of the development lifecycle, which are listed in table 1. The survey asked participants to select any practice that they found challenging to incorporate into their SDL. Participants were free to choose multiple practices when selecting those they found difficult. The survey responses for the practices that participants found challenging to implement are illustrated in figure 3.

Practice 1	Security management
Practice 2	Specification of security requirements
Practice 3	Secure by design
Practice 4	Secure implementation
Practice 5	Security verification and validation testing
Practice 6	Management of security-related issues
Practice 7	Security update management
Practice 8	Security guidelines

Table 1: IEC 62443-4-1 practices

As shown in figure 3, survey participants identified security management, secure by design, and security update management practices as the most challenging. Participants who selected a practice as difficult to implement had the opportunity to elaborate on their specific challenges through a freeform text question and verbal explanations during the meeting. Several recurring themes emerged from their responses.

After selecting the security management practice as a challenge, the participants voiced several concerns. This practice requires establishing a comprehensive SDL as part of the product development process and enforcing it across the organization for both existing and new projects makes it inherently complex. Another challenge highlighted was determining the applicability of specific requirements in the standard. For instance, participants noted difficulty in deciding when requirements, such as providing hardening guidelines, apply to their unique circumstances as industrial equipment manufacturers since often end users are not responsible for installation, hardening, or maintenance of industrial equipment on their own. Another significant issue was identifying and

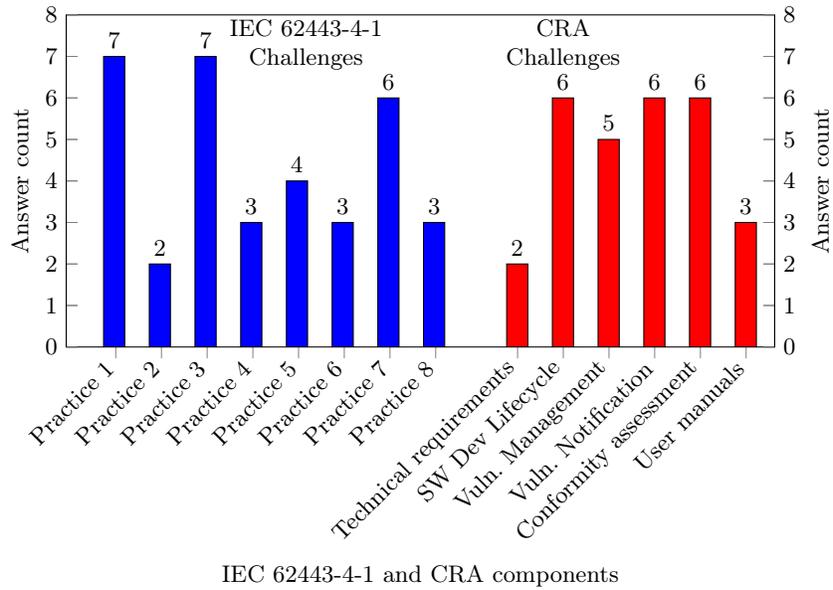


Fig. 3: Challenges with IEC 62443-4-1 and CRA requirements.

allocating responsibilities, as organizational structures often do not align with the process structures outlined in the standard. This misalignment necessitates negotiating additional responsibilities for teams and securing management buy-in at various levels. Communication gaps between management, developers, and cybersecurity teams were also frequently mentioned. Upper management often lacks sufficient understanding of cybersecurity requirements, while cybersecurity specialists sometimes struggle to effectively convey challenges and issues to leadership, leaving participants uncertain about how to address these communication barriers. Additionally, the practice mandates ensuring adequate security expertise and it was seen as a challenge, with participants citing a perceived shortage of qualified cybersecurity professionals. A perhaps subtle challenge that might have been missed is also the difficulty in evaluating whether personnel assigned to roles have the appropriate cybersecurity skills. Interestingly, participants did not report difficulties with the more technical controls within the security management practice 1, such as SM-6 (file integrity) or SM-8 (controls for private keys), suggesting that technical controls are generally perceived as less challenging compared to organizational and procedural aspects.

Participants identified a lack of cybersecurity-educated or experienced experts as a key challenge with the secure by design practice 3. They noted the difficulty of finding seasoned professionals who possess a broad understanding of defense-in-depth practices, such as least privilege, audit logging, and secure boot, while also being capable of collaborating with multiple product teams. Additionally, these experts must be able to dedicate sufficient time to thoroughly

document design reviews and assessments, further complicating the implementation of this practice.

Security update management practice evoked conversation on several challenges that survey participants face when aiming to comply. This is understandable, as many industrial equipment manufacturers rely on embedded software packages that are delivered as complete images, unlike desktop software libraries where individual patches can be built, delivered, and applied to address specific vulnerabilities. Furthermore, industrial equipment often has intermittent or no connectivity, making it difficult to meet timely update requirements. While the standard acknowledges that the availability and safety properties of industrial equipment take precedence over addressing theoretical vulnerabilities, participants still found compliance with the update management practice challenging. Finally, the end users of industrial equipment are often not qualified to access or apply updates. This creates a disconnect between the standard's requirements for security-update documentation and the practical realities of end-user capabilities.

Challenges in CRA Implementation

When exploring challenges with CRA compliance, we categorized the act's requirements into technical requirements, secure development lifecycle (SDL) requirements, vulnerability management, vulnerability notification, conformity assessment, and user manuals. Technical documentation, including risk assessments and interface descriptions, was not queried as a separate category but was considered part of a mature SDL. Participants were allowed to select multiple answers to indicate the areas they found challenging. The responses for each category of requirements are summarized in Figure 3.

The CRA requirement text "*Products with digital elements shall be designed, developed, and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks*" implies the need for a mature secure software development lifecycle (SDL). Many survey participants found this challenging, echoing the difficulties observed with IEC 62443-4-1 requirements discussed earlier. Establishing and enforcing an SDL across an organization is a substantial undertaking. Vulnerability notification requirements were also highlighted as a significant challenge, as many participants had little prior experience with such practices. The CRA deadline of notifying within 24 hours of an actively exploited vulnerability was perceived as stringent. Some participants even expressed doubts about their ability to detect actively exploited vulnerabilities promptly. Similarly, participants were uncertain whether their vulnerability management processes and tools were sufficiently mature to meet CRA expectations. Conformity assessment was another major area of concern. Participants were unsure whether their products required external assessment by a notified body or if internal self-declaration would suffice based on their product type. Even when self-declaration was deemed acceptable, participants questioned whether their quality teams, which currently oversee self-declaration and CE labeling, were adequately equipped to evaluate compliance with the cybersecurity requirements of the CRA. Finally, the pattern observed earlier repeated, the

technical requirements of CRA, such as confidentiality and integrity protection of stored and transmitted data, were not generally perceived as challenging.

Cost Impact and Organizational Changes When asked about the estimated cost impacts of CRA compliance, as evident in figure 4, 50% of participants expect costs to remain under 20%, 25% anticipate costs to increase by 20–40%, and, surprisingly, 25% foresee no cost impact at all. Similarly, when participants were asked about potential changes in employee roles, also shown in figure 4, the majority (50%) expect roles to remain unchanged after the CRA comes into force, while 33.3% anticipate role changes, and 16.7% remain uncertain. These findings suggest that CRA may not significantly impact employee roles or organizational costs. This could indicate that manufacturers are either reasonably prepared or have resigned themselves to achieving compliance using their existing resources without expecting additional budget or support for structural changes.

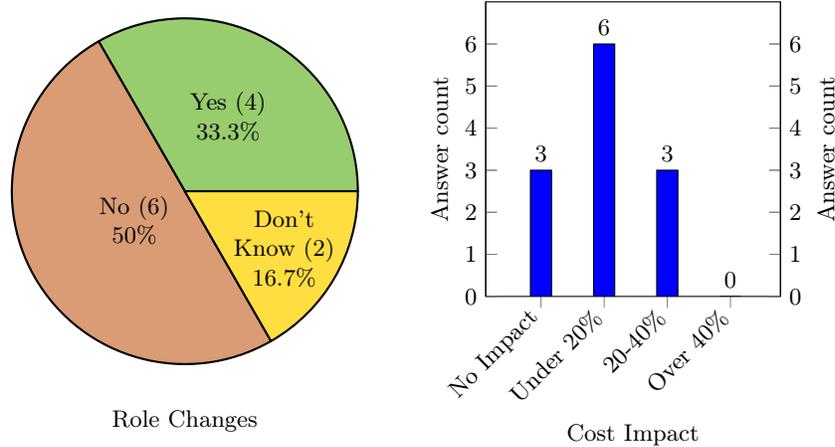


Fig. 4: Anticipated Role Changes and Cost Impact of CRA.

Transition period The questionnaire included a freeform question about whether the CRA transition period of 21 months for vulnerability notification requirements and 36 months for all other requirements is reasonable. The general consensus was that the transition period is reasonable, though some participants expressed concerns about uncertainty surrounding conformity assessment requirements. Additionally, some acknowledged that a longer transition period might not necessarily make compliance easier, as it could simply encourage companies to delay action until the last minute. One participant noted that while the transition period might seem reasonable on paper, it could prove insufficient without strong leadership commitment to the significant organizational changes required.

Use of open-source software To investigate any specific concerns related to open-source software, we included the following question in the survey: “*What impacts do you see on the use of open-source software in your products that need to comply with the CRA?*” Participants acknowledged that complying with the CRA would make the use of open-source software more complex. They emphasized the need for accurate SBOM tracking tools to detect and document all open-source components comprehensively. Additionally, participants highlighted the need for more rigorous vetting processes to ensure components are actively maintained and the necessity of establishing reliable channels for receiving vulnerability information.

Role of CRA in improving security posture When asked about their overall impressions of how significantly the CRA is expected to enhance the cybersecurity of their products, participants provided varied responses. While the majority leaned toward the belief that the act would improve the security posture of their products, a few participants expressed skepticism, with some stating they did not anticipate any tangible improvements. This suggests that while many manufacturers recognize the potential benefits of the CRA, not all perceive it as a guaranteed driver of enhanced cybersecurity. Some may regard the act as more of a regulatory burden than a practical means to improve product security.

6 Tackling CRA Challenges

As is evident from the survey results, industrial equipment manufacturers anticipate several challenges for CRA compliance. In this section, we focus on three key areas, and provide practical recommendations for tackling the challenges.

Cybersecurity Experts Several survey participants identified the shortage of qualified cybersecurity professionals as a critical challenge, particularly in the context of implementing IEC 62443-4-1 practices related to security management and secure-by-design principles. Article 10 of the CRA [8] acknowledges this issue but stops short of mandating specific actions. Instead, it encourages EU member states, ENISA, and the European Cybersecurity Competence Centre to develop “*organizational and technological tools to ensure sufficient availability of skilled professionals.*” Addressing this shortage requires broad, long-term planning. However, in the interim, industrial equipment manufacturers must prioritize internal training, upskilling, and adopting a shift-left strategy. This approach integrates security responsibilities across all teams, rather than confining them to a dedicated cybersecurity team.

Communication Survey participants highlighted several communication challenges at various levels, including the need for clear and effective communication between the cybersecurity team and leadership to convey the CRA’s extensive requirements, the number of affected products, required investment, management commitment, and the short transition timeline. Additionally, challenges arise between the cybersecurity team, which is well-versed in the SDL and technical requirements, and the quality team, which oversees self-declaration

and CE labeling. The quality team will need to collaborate with cybersecurity to verify CRA compliance and ensure technical documentation is complete before signing a self-declaration. Lastly, participants raised concerns about communication with external authorities, such as ENISA and national CSIRTs, when making vulnerability notifications.

To address communication challenges, it is essential to establish regular cross-departmental meetings involving the cybersecurity team, company leadership, and the quality team. These meetings should ensure alignment on CRA requirements, investment needs, and clearly define the roles and responsibilities of each organizational unit in achieving CRA compliance. Additionally, setting clear next steps and timelines will help streamline the process and foster effective collaboration. Training sessions and workshops tailored for the quality team can further build a shared understanding of CRA requirements. Establishing dedicated communication channels and implementing feedback mechanisms will also help mitigate anticipated communication challenges. Adopting a shift-left strategy will integrate security considerations early in the development process, ensuring that security becomes a shared responsibility across all teams. To address communication challenges related to vulnerability notifications, ENISA and national CSIRTs should prioritize developing a unified Coordinated Vulnerability Disclosure (CVD) ecosystem with clear communication practices and automated tools for streamlined disclosures.

Tooling To encourage discussion, not only on the challenges but also on potential techniques to overcome them, our survey included an optional freeform question: *What kind of tooling would help your organization in fulfilling the CRA requirements and realizing its full benefits?* Participants had many suggestions, which we synthesized into four tooling categories, along with specific recommendations that refine their preliminary thoughts.

Several participants expressed a desire for advanced, cost-efficient *DevSecOps* tools that support the entire development lifecycle, from threat modeling to requirements tracking, source code scanning, and penetration testing. While many tools are already available for such tasks, organizations should first study their existing development pipelines and understand how new projects and features are introduced and specified. It is crucial to ensure that the chosen *DevSecOps* tools can integrate seamlessly with these development pipelines. If the development pipelines do not align with modern *DevSecOps* principles, companies should reconsider and modify them accordingly.

The importance of *vulnerability management* tools was a recurring theme among participants. Many recognized the value of standard SBOM formats like CycloneDX [2] and tools for tracking vulnerabilities based on SBOM data. While vulnerability management tools are necessary and readily available, companies should also prepare for centrally aggregating vulnerabilities from multiple sources and constructing a hierarchy of vulnerabilities that accurately reflects the composition of their product components. Adopting the Common Vulnerability Scoring System (CVSS) for impact assessment is essential too. To reduce noise from false

positives or low-impact vulnerabilities, organizations should consider advanced risk-rating methods, including AI-driven analysis if necessary.

Governance Risk and Compliance (GRC) tools were also mentioned by a couple of participants. While GRC tools can be helpful, the primary goal for industrial equipment manufacturing companies should be setting a company-wide Cybersecurity Management System (CSMS) aligned with IEC 62443 if it hasn't already been done. Once the CSMS is developed, it needs to be put into practice, and GRC tools can help operationalize and monitor its implementation. However, ensuring that all the policies in the CSMS are understood by employees and effectively applied across the organization is a significant challenge that cannot be solved by GRC tools alone.

Participants also emphasized the necessity of *incident response and workflow automation* tools to comply with CRA notification responsibilities. For this, ENISA and national CSIRTs should develop a unified CVD policy that supports the use of protocols such as Structured Threat Information eXpression (STIX) [3] to automate the exchange of threat and vulnerability information and standard vulnerability reporting formats like the Common Vulnerability Reporting Framework (CVRF) [1]. Concurrently, organizations should prepare templates for initial, detailed, and final reports to streamline the notification process if and when an actively exploited vulnerability is discovered.

As a general recommendation for selecting tools to ensure CRA compliance, organizations should thoroughly evaluate the application programming interface (API) and integration support of each tool before adoption. This evaluation is crucial for building an end-to-end automated pipeline that spans from threat modeling to continuous penetration testing. Additionally, selecting tools with flexible licensing models that can scale with project needs is essential. Prior to making a commitment, organizations should pilot and verify that tools conform to organizational workflows. Lastly, engaging with peers at industry forums to share experiences and adopt best practices based on insights of others can enhance tool selection and implementation.

7 Conclusion

We conducted a survey of industrial equipment manufacturing companies to explore the challenges they anticipate as they prepare for CRA compliance. The survey revealed several key concerns, including the tight timelines for vulnerability notifications, the requirement to support timely automatic security updates with opt-out options, the need for updated user manuals, and the complexities associated with using open-source software. Through freeform discussions during the survey, participants shared ideas for addressing these challenges, which we have synthesized into practical recommendations across three critical areas: improving communication within organizations and among stakeholders, addressing the shortage of cybersecurity experts, and enhancing security tooling. These findings provide valuable insights that can help other companies assess whether their challenges align with those identified by their peers. This knowledge, along

with the practical recommendations, should support industrial equipment manufacturing companies, as well as other organizations, in proactively preparing for CRA compliance.

8 Acknowledgements

The authors gratefully acknowledge the partial funding provided by the Business Finland Veturi project *Cybersecurity Assurance for IEC62443 Based Environments (CTAC)*. We extend our sincere thanks to all the members of the CTAC project for their invaluable contributions. Additionally, we would like to express our gratitude to the participants of the study for their insightful feedback on CRA and the challenges it presents.

References

1. CVRF 1.1, <https://github.com/CVRF/cvrf1.1>
2. CycloneDX bill of materials standard, <https://cyclonedx.org/>
3. STIX documentation, <https://oasis-open.github.io/cti-documentation/stix/intro.html>
4. Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements (2018)
5. Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components (2019)
6. Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design (2020)
7. Lifts for the transport of persons and goods – Part 20: Cybersecurity requirements (2023)
8. Cyber resilience act (2024), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402847#d1e47-71-1, official Journal of the European Union, L 284/7
9. Center for Cybersecurity Policy and Law: Joint letter of experts on the EU cyber resilience act and vulnerability disclosure (October 2023), <https://www.centerforcybersecuritypolicy.org/insights-and-research/joint-letter-of-experts-on-cra-and-vulnerability-disclosure>, accessed: 2025-01-06
10. European Cyber Security Organisation (ECSO): Challenges of the industry to implement the CRA. Tech. rep. (March 2024), https://ecs-org.eu/ecso-uploads/2024/03/ECSO_Survey_CRA_2024.pdf
11. of the European Union, C.: Regulation of the european parliament and of the council on horizontal cybersecurity requirements for products with digital elements and amending regulation (eu) 2019/1020 (2023), <https://data.consilium.europa.eu/doc/document/ST-17000-2023-INIT/EN/pdf>
12. European Union Agency for Cybersecurity (ENISA): Cyber resilience act requirements standards mapping (November 2024), https://www.enisa.europa.eu/sites/default/files/2024-11/Cyber%20Resilience%20Act%20Requirements%20Standards%20Mapping%20-%20final_with_identifiers_0.pdf
13. Phipps, S.: The ultimate list of reactions to the cyber resilience act (2023), <https://opensource.org/blog/the-ultimate-list-of-reactions-to-the-cyber-resilience-act>

14. Schoo, P.: Navigating the CRA: A brief analysis of european cyber resilience act and resulting actions for product development. In: Proceedings of the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024). pp. 245–251. SCITEPRESS – Science and Technology Publications, Lda. (2024). <https://doi.org/10.5220/0012690500003705>
15. Szedlak, C., Reinemann, H., Hatzelmann, S.: Ensuring cybersecurity compliance: Assessing SME awareness and preparedness for the cyber resilience act. In: 5th Asia Pacific Conference on Industrial Engineering and Operations Management. IEOM Society International, USA, Tokyo, Japan (September 2024). <https://doi.org/10.46254/AP05.20240160>
16. Thiel, M.: Challenges and opportunities of the eu cyber resilience act. Risk Management Magazine (August 2024), <https://www.rmmagazine.com/articles/article/2024/08/08/challenges-and-opportunities-of-the-eu-cyber-resilience-act>