Applied Human Factors and Ergonomics (AHFE2025), Vol. 199, 2025, 2291–2301
https://doi.org/10.54941/ahfe1007041

Coordinating Asset Owner and PSIRT for CRA Vulnerability Recognition: Evidence-Based Mechanisms From Coordination Theory

Jumpei Tahara[1,2] and Kenji Watanabe[1]

[1]Nagoya Institute of Technology, Gokiso-cho, Showa-Ku, Nagoya, Aichi, 466–8555 Japan
[2]Manufacturing and Innovation DX Laboratory, Nagoya Institute of Technology, Gokiso-cho, Showa-Ku, Nagoya, Japan

ABSTRACT

The EU Cyber Resilience Act (CRA) requires manufacturers to provide early warning within 24 hours, detailed notification within 72 hours, and final reporting within 14 days after corrective measures become available, upon becoming aware of actively exploited vulnerabilities (Article 14). However, the evidence necessary to establish awareness exists primarily in asset owner environments, and asset owners bear no reporting obligation. This creates a structural coordination challenge: manufacturers require evidence they cannot independently access, and fixed reporting deadlines commence upon awareness. This study applies Malone & Crowston's coordination theory to identify three dependency relationships: bidirectional knowledge asymmetry (producer-consumer relationship) between asset owners who hold evidence and PSIRTs who hold product knowledge; time allocation (shared resource) under fixed reporting deadlines (24h/72h/14d); and misalignment between different objectives (task-subtask dependency). We propose a three-layer mechanism for managing these dependencies. C0 (Reachability) provides reporting channels. C1 (Evidence Coordination Profile) decomposes Article 3(42) awareness definition into five propositions and structures evidence into four categories (E1-E4), enabling the establishment of awareness and phased reporting. C2 (Incentive Design) converts asset owners' voluntary cooperation into organizational security improvement through three benefits. These three mechanisms mutually reinforce each other to achieve continuous coordination. Theoretically, this extends the coordination theory to regulatory compliance contexts in which coordination is voluntary. Practically, it provides implementable guidance for manufacturers facing CRA enforcement by 2027.

Keywords: Cyber resilience act, PSIRT, Coordination theory, Vulnerability recognition, Reporting obligation, Voluntary cooperation, Evidence-based coordination

INTRODUCTION

Regulatory Context and Compliance Challenge

The EU Cyber Resilience Act (CRA, Regulation 2024/2847) was published on October 20, 2024, marking a fundamental shift in the cybersecurity

regulation for digital products. While the majority of the regulation became applicable from December 11, 2027, the reporting obligations under Article 14 became applicable from September 11, 2026. Non-compliance with mandatory cybersecurity requirements and reporting obligations by manufacturers is subject to penalties of up to €15 million, or 2.5% of the total worldwide annual turnover (Article 64(2)). The CRA imposes secure development lifecycles, vulnerability management, and reporting obligations—the focus of this study—on manufacturers of products ranging from consumer IoT to industrial control systems.

Article 14: Departure From Existing Standards Through Fixed Time Windows

Article 14 mandates manufacturers to provide three-stage reporting with fixed deadlines for actively exploited vulnerabilities: early warning within 24 h of awareness, detailed notification within 72 h, and final report within 14 days after corrective measures become available (Article 14(2)). This study refers to these as "fixed windows (24h/72h/14d)".

These fixed windows represent a fundamental departure from existing standards. ISO/IEC 29147:2018 recommends acknowledgment within seven days of receipt, but subsequent deadlines are left for market-driven negotiations. IEC 62443-4-1:2018 also considers response to be "driven by market forces." In these standards, the trigger point is the receipt of a vulnerability report, and the trigger is the existence of a vulnerability, regardless of active exploitation.

In contrast, the trigger point of CRA Article 14 is the moment of becoming aware of active exploitation, and the trigger is the occurrence of exploitation, as defined in Article 3(42). The regulation defines "actively exploited vulnerability" as "a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner." Recital 68 specifies this as "the occurrence of a security breach attributable to a defect in the manufacturer's product." This definition contains two elements of proof: causality (breach is attributable to a product defect) and maliciousness (unauthorized access).

Figure 1 illustrates the timeline of this report. From Ti (incident occurrence) through Tr (report receipt) to T0 (establishment of awareness of active exploitation), fixed windows begin at T0. From T0, T24h (early warning) is required within 24 h, T72h (detailed notification) within 72 h, and Tm + 14d (final report) within 14 days from Tm (corrective measure available).

Operational Challenge: The Undefined "Awareness"

As shown in Figure 1, the fixed windows begin from T0 (the moment of establishing awareness of active exploitation). However, the operational challenge of the regulation lies in the fact that "becoming aware' that triggers T0 is undefined (Article 14(2)). While the 24h/72h/14d deadlines are explicit, the moment when the window opens—namely, the transition condition from

Tr to T0—is legally ambiguous, and its operational definition is left to the manufacturer's interpretation.

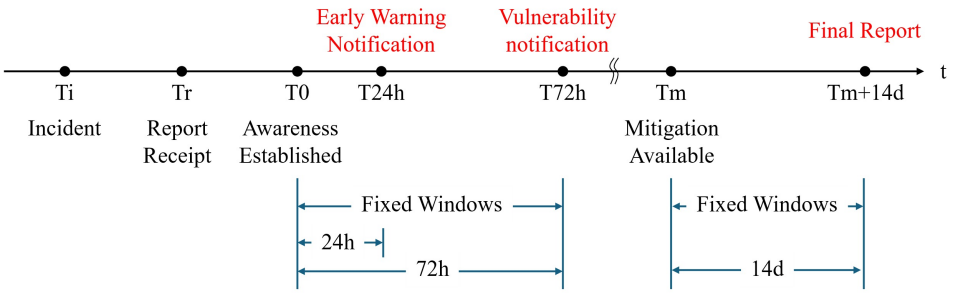

Figure 1: CRA article 14 reporting timeline.

Interpreting awareness as the moment of incident report receipt (Tr=T0) imposes unrealistic burdens on manufacturers, while interpreting it as the moment of complete analysis completion invites reporting delays (Tr<<T0).

This study adopts an intermediate interpretation: awareness is established at the moment of completing minimum scrutiny, when the manufacturer confirms product applicability and exploitation facts (a scrutiny process exists during Tr->T0). This interpretation is consistent with Article 3(42) requirement for "reliable evidence," while recognizing that comprehensive analysis within 24 hours is impossible. This scrutiny process itself requires coordination with asset owners, because the necessary evidence exists primarily in asset-owner environments.

Evidence Location and Necessity of Coordination

Evidence to establish active exploitation, such as incident logs, network configurations, and intrusion detection records, exists primarily in asset-owner environments. This study's "asset owner" refers to the organization that owns and manages the system where the incident occurred and holds the evidence (corresponding to "system owner" in CRA Article 3(42) and "asset owner" in IEC 62443).

Manufacturers lack direct observability for products deployed in industrial automation environments or enterprise networks. They cannot independently verify whether anomalies stem from vulnerabilities in their products, configuration errors, or unrelated incidents and cannot distinguish unauthorized access from legitimate testing without the asset owner context.

This creates fundamental information asymmetry: asset owners hold evidence but lack product knowledge, while manufacturers hold product knowledge but lack evidence. Establishing awareness requires the integration of complementary knowledge across organizational boundaries. The urgency of the fixed 24h/72h windows transforms this into a time-critical coordination challenge.

Research Positioning and Contribution

Ruohonen and Timmers (2025) analyzed the CRA's vulnerability coordination requirements and mapped reporting flows from manufacturers to CSIRTs and ENISA after awareness. However, their analysis began after awareness was established, leaving the pre-awareness coordination process unexamined. This study fills this gap by focusing on the asset owner-product Security Incident Response Team (PSIRT) coordination necessary for establishing awareness.

In this study, "PSIRT" refers to the specialized organizational unit within the "manufacturer" of the CRA text responsible for receiving vulnerability reports and determining awareness (FIRST PSIRT Services Framework). The scope includes industrial control systems (IEC 62443 domain) and enterprise network equipment. These manufacturers are expected to comply with the vulnerability management processes (Practice 6: Defect Management) defined by IEC 62443-4-1, but in establishing the "awareness" required by the CRA, evidence collection from asset owner environments is indispensable. Because these are deployed in asset-owner environments and manufacturers cannot directly observe deployment environments, explicit coordination mechanisms are required.

Research Questions

RQ1: From a coordination theory perspective, what dependencies hinder the establishment of awareness between asset owners and PSIRTs under CRA's fixed time constraints?

RQ2: How should coordination mechanisms be designed to manage the identified dependencies?

RQ3: How do the proposed mechanisms address the situation in which asset owners bear no reporting obligations?

This analysis is based on the CRA text (Regulation (EU) 2024/2847) enacted on October 23, 2024, and published in the Official Journal on November 20, 2024. Delegated acts indicated in Article 14(6) and operational definitions of "awareness" may be clarified in the future. Although this study's interpretation is based on the current text, adjustments may be required with the emergence of complementary regulations.

THEORETICAL FOUNDATION

Coordination Theory Framework

This study is grounded in Malone and Crowston's (1994) coordination theory. Coordination theory defines coordination as "managing dependencies among activities" and provides a framework for systematically analyzing types of dependencies and coordination processes. Achieving CRA reporting obligations requires continuous coordination between PSIRTs and asset owners; however, structural barriers exist. Asset owners lack product knowledge and PSIRTs lack access to on-site information. Furthermore, asset owners bear no reporting obligations under the CRA, and lack incentives

to cooperate. Analyzing these through the coordination theory framework reveals the following dependencies.

First Dependency: Producer-Consumer Dependency

According to Malone and Crowston (1994), producer-consumer relationships have multiple dependency aspects: (1) prerequisite constraints—PSIRTs cannot begin analysis until asset owners complete evidence collection; (2) transferevidence must be transferred from asset owner environments to PSIRT environments; and (3) usability—evidence must be usable for PSIRTs' causality and maliciousness determinations.

Second Dependency: Shared Resource

Asset owners and PSIRTs share limited resources. Asset owners must allocate time between incident response and evidence collection, whereas PSIRTs must allocate time to processing multiple reports. CRA Article 14(2)'s 24h/72h deadlines impose exogenous constraints on the resource allocation. Fixed deadlines are non-negotiable and commence at the moment awareness is established (T0). This exogenous nature is fundamentally different from traditional disclosure timelines (ISO/IEC 29147:2018). Traditionally, manufacturers can negotiate flexible timeframes, but the CRA imposes fixed windows. Although there are no time constraints before awareness (Ti->T0) because fixed windows commence at the moment of awareness establishment, pre-awareness coordination efficiency determines post-awareness reporting quality.

Third Dependency: Task-Subtask

When a larger goal is decomposed into multiple subtasks, task-subtask dependency relationships exist. According to Malone and Crowston, this dependency involves both goal selection and task decomposition. The superordinate goal of achieving CRA compliance is decomposed into multiple subtasks: evidence collection (handled by asset owners), awareness determination (handled by PSIRTs), and reporting (handled by PSIRTs).

However, asset owners and PSIRTs are independent organizations, and asset owners bear no reporting obligations under the CRA. The primary goals of asset owners are incident resolution and system recovery, while PSIRTs' primary goal of PSIRTs is CRA regulatory compliance and protection of other asset owners. Malone and Crowston note that coordination, incentives, motivations, and emotions are extremely important in human systems. To align these different goals with the shared sub-goal of "rapid and accurate awareness establishment," an incentive design that creates bidirectional benefits is necessary.

COORDINATION MECHANISMS DESIGN

This section proposes the coordination mechanisms C0 (Reachability), C1 (Evidence Coordination Profile), and C2 (Incentive Design)to manage the three dependencies identified in the previous section. Figure 2 shows how

these mechanisms support the overall coordination process (Ti->Tm + 14d) and mutually complement each other.

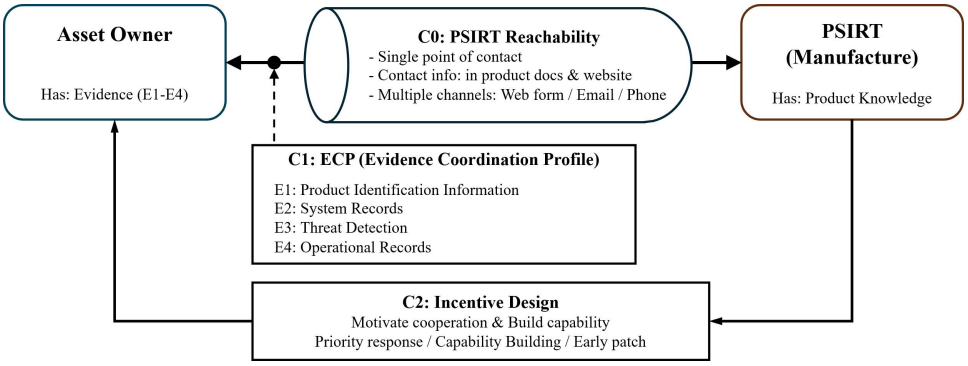

Figure 2: Mutually reinforcing coordination mechanisms for vulnerability recognition.

C0: PSIRT Reachability

The C0 mechanism manages the transfer dependency of the producer-consumer relationship. Article 13 (17) of the CRA mandates manufacturers to designate "a single point of contact that users can easily identify" to facilitate vulnerability reporting. This regulatory requirement explicitly states the importance of asset owners being able to discover PSIRTs when incidents occur.

C0 provides multiple reporting channels (web form, email, phone) in compliance with ISO 29147:2018 and publishes the contact information required by the CRA in product documentation and corporate websites. This enables asset owners to rapidly reach from Ti (incident occurrence) to Tr (PSIRT contact). C0's primary function is to provide a pathway for transferring the evidence structure defined by C1.

Structured reporting forms corresponding to the ECP's four categories enable asset owners to systematically provide evidence necessary for the establishment of awareness (Ti->T0), and continuous information exchange through the same channel remains possible after awareness (post-T0).

C1: Evidence Coordination Profile (ecp)

- **Purpose of C1 and Dependencies Managed**
  The C1 mechanism manages the prerequisite constraint and usability dependencies of the producer-consumer relationship, as well as the shared resource (time) dependency. By clearly defining "evidence necessary for awareness," it enables asset owners to understand what to collect and PSIRTs to make awareness determinations based on consistent criteria. Evidence standardization ensures usability and allocates time for evidence collection considering the CRA's phased reporting requirements.

- **Decomposition of Article 3(42) and Elements of Proof**
  Formalizing Article 3(42), awareness establishes proof of P1^P2^P3^P4^P5. P1 indicates that vulnerability exists in the product (product applicability), P2 indicates that the product is deployed in the

target environment (environment applicability), P3 indicates that the vulnerability is exploited in the system (exploitation fact), P4 indicates that it is by a malicious actor (maliciousness), and P5 indicates that it is without the system owner's permission (unauthorized). P1^P2^P3 collectively establish the causality required by Recital 68 (the breach is attributable to a product defect). P1 demonstrates that a vulnerability exists in the product, P2 demonstrates that the product exists in the environment, and P3 demonstrates that exploitation occurred; when these are assembled, the causal relationship that "the breach is attributable to the defect in that product" is established.

- **Evidence Structure for T0 Awareness Establishment**
  C1 structures to prove P1-P5 into four categories (Table 1). This structuring enables asset owners and PSIRTs to organize evidence within a common framework and streamline the Ti→T0 awareness establishment process.

Table 1: Evidence coordination profile (ECP) for T0 awareness establishment.

Category	Corresponding Propositions	Required Information Examples
[E1] Product identification information	P1: Product applicability	Product name, version
[E2] System records	P2: Environment applicability P3: Exploitation fact	Product logs, communication logs, network configuration
[E3] Threat detection	P4: Maliciousness	Security tool detection
[E4] Operational records	P5: Unauthorized	Work schedules, change records

- **Deductive Derivation of Evidence Categories**
  P2 (environmental applicability) and P3 (exploitation fact) can be proven from the same evidence in practice. System records collected by asset owners contain both information showing that the product was deployed in the environment (IP addresses, network configurations, etc.), and information showing that the vulnerability was exploited in that environment (anomalous access patterns, unauthorized authentication attempts, etc.). Exploitation of vulnerability implies that the product is deployed in an environment where exploitation is possible. Therefore, C1 defines E2 (System Records) by integrating P2 and P3; for P1, P4, and P5, independent categories (E1, E3, and E4) were established.

  E1 (Product Identification Information) includes the product name and version, enabling PSIRTs to cross-reference with known vulnerabilities. E2 (System Records) includes product logs, network logs, communication records, and network configuration. While asset owners cannot determine "whether this is attributable to a product defect," they can record "what happened." PSIRTs cross-reference this with product knowledge to determine P2 and P3.

E3 (Threat Detection) includes the detection results from IDS/SIEM/AV, etc. However, not all asset owners are deployed, and they may be limited, especially in small and medium-sized enterprises. PSIRTs can infer E2 maliciousness when E3 is unavailable. E4 (Operational Records) includes work schedules and system change records, confirming that the observed events were not approved work. If no corresponding records exist, the event is determined to have occurred "without permission."

- **Reporting Stages After T0 Awareness Establishment**
  The ECP of C1 adopts the "as available" principle corresponding to Article 14(2)'s phased reporting requirements (24h/72h/Tm + 14d). E1 (Product Identification Information) provides the minimum information necessary for T24h reporting. E2 (System Records) has a high collection burden for asset owners during an incident response but can be obtained incrementally from existing log management systems. E4 (Operational Records) can determine unauthorized (P5) by checking the management of change or permitting work records that are standard operations in industrial environments. E3 (Threat Detection) requires specialized analysis or security tools, so it can be supplemented incrementally after T72h. This phased approach is consistent with Article 14(2)(b), permitting "as available" for 72-hour reporting.

C2: Voluntary Cooperation Incentive Design

- **Purpose of C2 and Dependencies Managed**
  The C2 mechanism manages goal alignment in task-subtask dependency. Because asset owners bear no reporting obligation under the CRA, an incentive structure that encourages voluntary cooperation is indispensable for PSIRTs to obtain evidence necessary for awareness establishment.

- **Incentive Asymmetry and Its Resolution**
  An incentive asymmetry exists between asset owners and PSIRTs. PSIRTs need evidence to fulfill Article 14 'sreporting obligations, but asset owners gain no direct benefit from cooperation. C2 resolves this asymmetry by providing the following benefits: (1) priority incident response; (2) technical capability improvement support (log collection automation, configuration review, etc.); and (3) early patch access. Through these, asset owners can convert cooperation into an improvement in their organization's security. In particular, (2) technical capability improvement support creates a virtuous cycle in which asset owner security capability is incrementally built through continuous cooperation, enabling the provision of higher quality evidence in the future.

- **Contractual Integration and Implementation Examples**
  Implementation methods for incentive structures depend on existing relationships with the asset owners. For customers with maintenance contracts, integration as technical support (priority incident response, configuration review, automation tool provision, etc.) within existing

contractual frameworks enables implementation without requiring additional organizational structures. For asset owners without maintenance contracts, a selective approach can be considered: publishing reporting protocols and expected evidence categories (ECP) on websites, and for significant vulnerability reports, providing technical support and early patch access individually. Such phased support systems have already been implemented in existing PSIRT practices (e.g., Cisco PSIRT) in the form of technical support via (Technical Assistance Center) for contract customers and the provision of reporting channels and free security updates for non-contract customers (Cisco, 2025).

C0-C2: Mutual Complementarity of Mechanisms

These three mechanisms form complementary structures. The reachability channel provided by C0 becomes the pathway for transferring evidence defined by C1, and structured reporting forms correspond to the ECP's four categories, enabling asset owners to systematically provide the necessary evidence. The ECP of C1 objectively defines "cooperation content" in C2's incentive structure, clarifying what level of cooperation is subject to benefits. The incentive of C2 motivates evidence provision according to C1 and promotes continuous exchange through C0.

Furthermore, technical support provided by C2 incrementally improves asset owners' capability to collect more complete ECP evidence for high-burden evidence categories, such as E2 (System Records). Technical capability improvement support, such as log collection automation and configuration review, enables the efficient collection of E2 even during an incident response. Through this virtuous cycle, asset owners (1) know "where" to report via C0, (2) know "what" to report via C1, (3) understand "why" to report via C2, and (4) become able to report "better" through C2. This mutual complementarity achieves continuous coordination throughout the entire period from Ti to Tm + 14d.

DISCUSSION

This study addressed the following three research questions:

RQ1: By applying coordination theory, we identified three dependencies. First, producer-consumer relationships: bidirectional knowledge asymmetry where asset owners hold evidence, but PSIRTs hold product knowledge, creates challenges in evidence transfer, usability, and prerequisite constraints. Second, shared resource (time): under CRA's fixed windows (24h/72h/14d), asset owner evidence collection delays compress PSIRT analysis time. Third, task-subtask dependency: Asset owners bear no reporting obligation and have different goals—organizational security improvement versus PSIRT's reporting obligation fulfillment.

RQ2: Three-layer mechanisms, C0 (Reachability), C1 (Evidence Coordination Profile), and C2 (Incentive Design), were proposed. C0 manages the transfer dependency through ISO/IEC 29147:2018-compliant reporting channels. C1 decomposes Article 3(42)'s awareness definition into P1-P5 and structures evidence into four categories (E1: Product

Identification, E2: System Records, E3: Threat Detection, E4: Operational Records). Through "as available" principle, E1 provides minimum information for T24h, E2/E4 enable incremental collection from existing records and logs, and E3 requires specialized analysis supplementable post-T72h, enabling awareness establishment and phased reporting within fixed windows. C2 manages goal alignment through three benefits (priority response, technical support, and early patch), thereby resolving incentive asymmetry. These mutually complement C0 pathways transfer C1 evidence, and C2 promotes C1 evidence collection.

RQ3: C2's incentive design motivates the voluntary cooperation of asset owners with no reporting obligation. These three benefits enable the conversion of cooperation into organizational security improvement, with technical support incrementally building evidence collection capability through continuous cooperation, enabling higher-quality C1 evidence provision. C0's adoption of ISO/IEC 29147:2018 requirements enables integration into existing maintenance contracts, allowing manufacturers to satisfy CRA requirements while leveraging the existing security infrastructure.

LIMITATIONS AND FUTURE RESEARCH

This study has the following limitations as theoretical research. First, while C1's ECP defines four evidence categories, the reliability evaluation procedures within each category (source verification, collection method validity, and completeness confirmation) require refinement through validation in practical environments. Second, the feasibility of 24-hour constraints, effectiveness of C2 incentives, and quantitative analysis of implementation costs remain unvalidated. Third, information asymmetry and moral hazard between asset owners and PSIRTs require analysis using agency theory (Jensen & Meckling, 1976). Benefit value evaluation and cooperation cost quantification are future empirical research issues. Fourth, the feasibility of small-to-medium scale PSIRTs providing C2 technical support and their effectiveness for asset owner capability building requires empirical verification.

For empirical research, tabletop exercises (TTX) are given the highest priority. Considering the constraints on obtaining actual data after the CRA implementation, TTX constitutes a realistic means of verifying the proposed mechanisms. Diverse asset owners (large enterprises and SMEs) and PSIRTs participate in hypothetical scenarios to verify (1) the necessity and feasibility of ECP four-category evidence, (2) the effectiveness of C2 incentives, and (3) the feasibility of coordination under 24-hour/72-hour constraints. Interview surveys with PSIRT practitioners and industrial control system operators will clarify practical barriers and facilitating factors. As theoretical extensions, the optimization of incentive parameters based on agency theory and the development of probabilistic models quantifying the reliability of each evidence category are required.

CONCLUSION

The EU Cyber Resilience Act requires manufacturers to provide initial reporting within 24 hours, but evidence necessary for awareness establishment is held by asset owners, who bear no reporting obligation. This study proposed three-layer mechanisms based on coordination theory—C0 (Reachability), C1 (Evidence Coordination Profile), and C2 (Incentive Design)—for this structural challenge. The ECP of C1 decomposes Article 3(42) awareness requirement into propositions P1-P5 and structures evidence into four categories (E1-E4), enabling T0 awareness establishment and phased reporting. C2 motivates asset owners' voluntary cooperation through three benefits: priority incident response, technical capability improvement support, and early patch access. These mutually complement each other, and achieve continuous coordination under fixed time constraints. This study pioneered a new application domain of coordination theory through a specific incentive design that enables coordination with external organizations bearing no reporting obligations. This study provides implementable guidance for manufacturers facing CRA enforcement that satisfies regulatory requirements while leveraging the existing security infrastructure. Empirical validation of the proposed mechanisms is urgently required for full CRA enforcement in 2027.

ACKNOWLEDGMENT

This work was partially supported by the Information-Technology Promotion Agency, Japan; however, all the remaining errors belong to the authors.

REFERENCES

Cisco. (2025). Security Vulnerability Policy. Website: https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html.

European Parliament and Council. (2024). Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Official Journal of the European Union, L, 2024/2847.

FIRST. (2022). PSIRT Services Framework Version 1.1. Forum of Incident Response and Security Teams. Website: https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1.

IEC. (2018). IEC 62443–4-1:2018 Security for industrial automation and control systems – Part 4–1: Secure product development lifecycle requirements. Geneva: International Electrotechnical Commission.

ISO/IEC. (2018). ISO/IEC 29147:2018 Information technology — Security techniques—Vulnerability disclosure. Geneva: International Organization for Standardization.

Jensen, M. C., Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360.

Malone, T. W., Crowston, K. (1994). The interdisciplinary study of coordination. ACM Computing Surveys, 26(1), 87–119.

Ruohonen, J., Timmers, P. (2025). Vulnerability coordination under the Cyber Resilience Act. arXiv preprint arXiv:2412.06261v2. Website: https://arxiv.org/abs/2412.06261.