Human Factors in Design, Engineering, and Computing, Vol. 238, 2026, 2551–2559
https://doi.org/10.54941/ahfe1008480

Cyber Resilience Act Reporting Obligations in Vulnerability Handling: An IDEF0 Analysis

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

Article 14 of the Cyber Resilience Act (CRA) requires manufacturers to report actively exploited vulnerabilities once they become aware of them, even while investigation and remediation development continue. We examine what information CRA reporting requires from existing vulnerability handling activities and which internal responsibilities manufacturers must assign. Using IDEF0, we map selected CRA provisions onto the six activities of ISO/IEC 30111, with ISO/IEC 29147 as a complementary reference. FIRST's PSIRT Services Framework v1.1 and IEC 62443-4-1:2018 inform the role analysis. Reporting may be required before remediation is complete, while subsequent reports require updates from development and release. The examined documents describe technical and communication roles but do not assign CRA reporting and user-information tasks to specific internal roles. This study identifies these information dependencies and the responsibilities that manufacturers must assign internally. Their operational feasibility remains to be evaluated in organizations.

Keywords: Cyber resilience act, Vulnerability handling, IDEF0, PSIRT, Responsibility allocation

INTRODUCTION

Manufacturers handle product vulnerabilities through activities including report receipt, verification, remediation development, and release (ISO/IEC, 2018, 2019). Coordinated vulnerability disclosure (CVD) involves exchanging information among stakeholders and agreeing on what to disclose and when. Alongside these activities, Article 14 of the Cyber Resilience Act (CRA), applicable since September 11, 2026, requires manufacturers to report actively exploited vulnerabilities to authorities in stages and inform users (European Parliament and Council, 2024). Authority reporting may therefore be required while investigation and remediation development continue.

Related Work

Ruohonen and Timmers (2025) examined CRA coordination between manufacturers and public authorities. Tahara and Watanabe (2025) studied dependencies and coordination mechanisms for evidence sharing between

Received October 16, 2026; Revised November 22, 2026; Accepted November 28, 2026; Available online December 1, 2026

© 2026 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

asset owners and product security incident response teams (PSIRTs). Tahara et al. (2025) identified collaboration difficulties between product safety teams and PSIRTs within manufacturers. These studies address coordination among stakeholders but do not directly examine the information CRA reporting requires from existing handling activities or the internal responsibilities that manufacturers must assign.

Problem Statement

Public disclosure schedules coordinated through CVD differ from CRA reporting deadlines. CERT/CC normally plans disclosure 45 days after the initial report to CERT/CC, even without a fix, but may adjust the date for circumstances such as active exploitation (CERT/CC, n.d.). By contrast, CRA Article 14 requires an early warning within 24 hours and a vulnerability notification within 72 hours of the manufacturer becoming aware of active exploitation. Authority reporting may thus be due while disclosure coordination and remediation development continue.

Assessing reportability requires exploitation evidence; subsequent reports also require information about the progress and availability of measures. The teams holding this information may differ from those deciding, authorizing, and submitting reports. We therefore examine these information dependencies and distinguish the roles established in the documents from responsibilities that manufacturers must assign internally.

Research Questions and Contribution

RQ1: What information dependencies connect CRA Article 14 reporting to existing vulnerability handling activities?
RQ2: Which roles and responsibilities do the examined documents establish for reporting and user information, and which internal assignments remain for manufacturers to determine?

We map CRA requirements onto six activities based on ISO/IEC 30111 and ISO/IEC 29147 and use IDEF0 to show reporting dependencies. By distinguishing documented roles from internal assignments, we identify the information connections and responsibilities needed to integrate regulatory reporting into existing vulnerability handling.

METHODS

The baseline comprises the six activities in ISO/IEC 30111:2019, Clauses 7.1.2–7.1.7, with corresponding activities and disclosure provisions from ISO/IEC 29147:2018. European draft prEN 40000-1-3 also addresses vulnerability handling (BSI, 2025). We use the published international standards to examine Article 14 reporting dependencies against existing handling activities.

We trace vulnerability handling from the receipt of a potential vulnerability report and map CRA Articles 3(42), 14(1), (2), and (6)–(8), 15(4), and 16(1). Severe-incident reporting under Article 14(3)–(5), Article 13, and Annex I are outside the scope. FIRST's PSIRT Services Framework v1.1 and IEC 62443-4-1:2018 support the role analysis (FIRST, 2020; IEC, 2018). Commission guidance informs the discussion of awareness.

IDEF0 represents information and constraints between activities (NIST, 1993). To compare reporting with the six existing activities, we place reportability assessment and reporting at verification (A3). This is an analytical choice, not a CRA requirement concerning internal activity placement or performers. IDEF0 arrows express functional dependencies rather than a fixed execution sequence.

Following Davaadorj (2018, pp. 32–36, 63) and Iwasaki (2021, pp. 40–46), we extract actors, actions, objects, and conditions. We retain source locations and modal verbs, split statements supporting multiple relationships, and distinguish explicit requirements from inferred links. We also distinguish the legal duty holder from the internal performer: a reporting duty addressed to the manufacturer does not establish a PSIRT assignment.

We classify the extracted content by its use in an activity: inputs are processed information, controls govern the activity, outputs are its results, and mechanisms are supporting people or resources. We then identify whether an output supplies another activity's input, control, or mechanism. The register records source clauses, activity and ICOM assignments, inferred links, and decisions to draw, aggregate, or omit model elements. Table 1 illustrates the mapping; Table 2 identifies the responsibilities manufacturers must assign for reporting and user information.

Table 1: Source statements and model elements.

Source Statement	Interpretation	Model Representation
30111 6.2.2, 6.3: policy setting by top management is recommended; internal policy defines responsibilities.	Top management establishes policy, which governs handling activities.	Management (M5) → A1 (M). Policy leaves A1 (O) and governs A2–A6 (C).
30111 6.5.3.3: customer support may receive reports, supported by processes and training.	Support staff perform receipt conditionally; training is an execution condition.	Support (M3) → A2 (M); reports → A2 (I).
CRA 14(2)(c), (c)(iii): final report with details of available measures.	Duty and conditions are explicit; internal performer is unspecified. A5 as provider is inferred.	A3 → O4; deadline → A3 (C); A5 → A3 (I). Exception for information already provided is recorded.

RESULTS

Figure 1 shows the manufacturer's vulnerability handling context (A-0).

Figure 2 shows the six ISO-based activities in an FEO diagram (A0F), while Figure 3 decomposes Figure 1 into an A0 diagram incorporating CRA reporting. Figures 2 and 3 use the same activity positions; bold arrows and "+" mark the CRA overlay, which also draws on existing handling information.

C1 represents standards, existing policies, embargoes, contracts, and law. The internal handling policy produced at A1 separately controls A2–A6. C2 represents CRA reporting conditions, deadlines, and requests from a computer security incident response team (CSIRT). M1–M5 denote PSIRT, product division, customer support/public relations, legal support, and management, respectively.

Reports received at A2 are verified at A3; confirmed vulnerabilities inform remediation development at A4, and we map assessment and remediation information to release at A5. Case updates from A6 may return to A3 or A4. Reports judged not to concern a vulnerability may leave handling at A3 after stakeholders are notified (30111 7.1.4, 7.1.7; 29147 6.3).

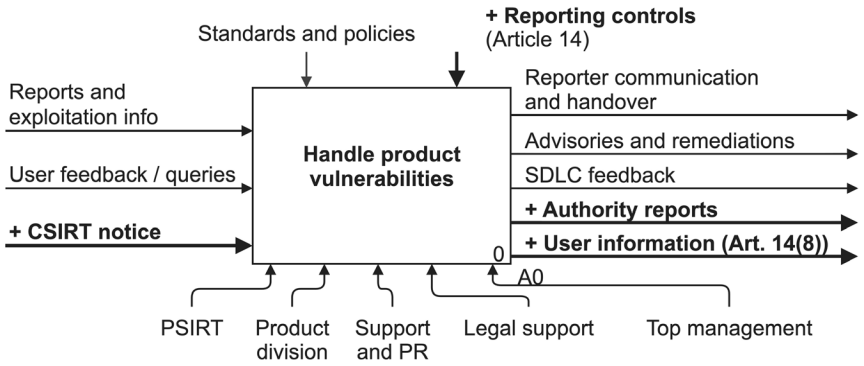


Figure 1: Vulnerability handling context.

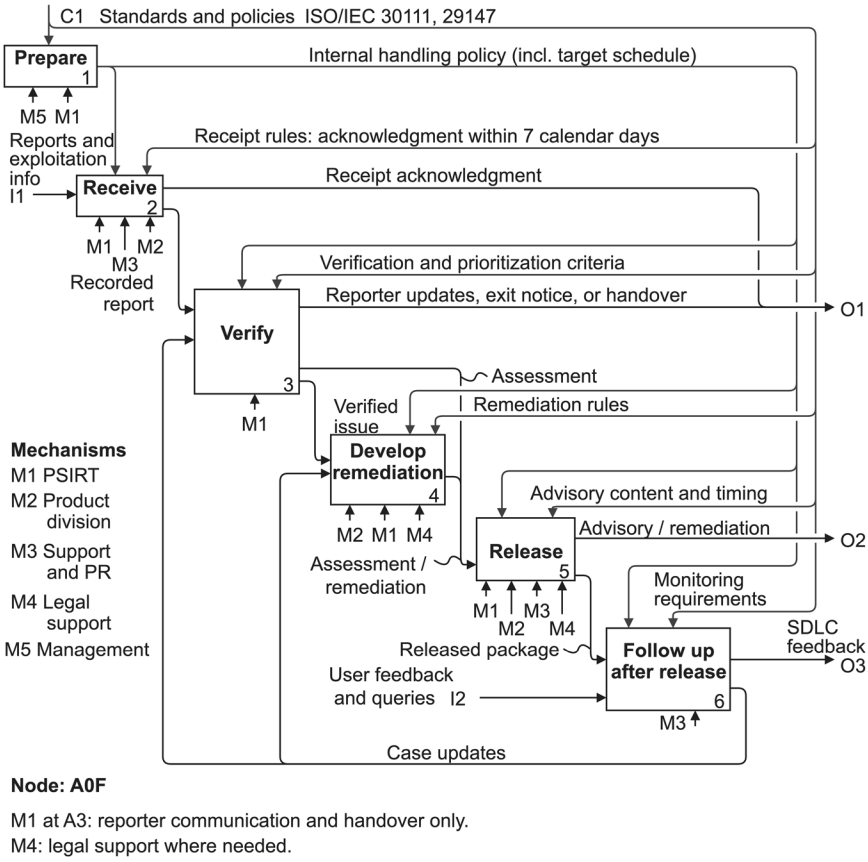


Figure 2: Baseline vulnerability handling.

Information Needed for Reporting

Figure 3 adds reportability assessment and reporting at A3. CRA Article 3(42) defines an actively exploited vulnerability by reliable evidence of malicious exploitation; Article 14(1) makes manufacturer awareness the reporting trigger. We represent CSIRT notices following third-party notifications under Article 15(4) as input I3 to A2, and authority reports (O4) and user information (O5) under Article 14 as outputs from A3.

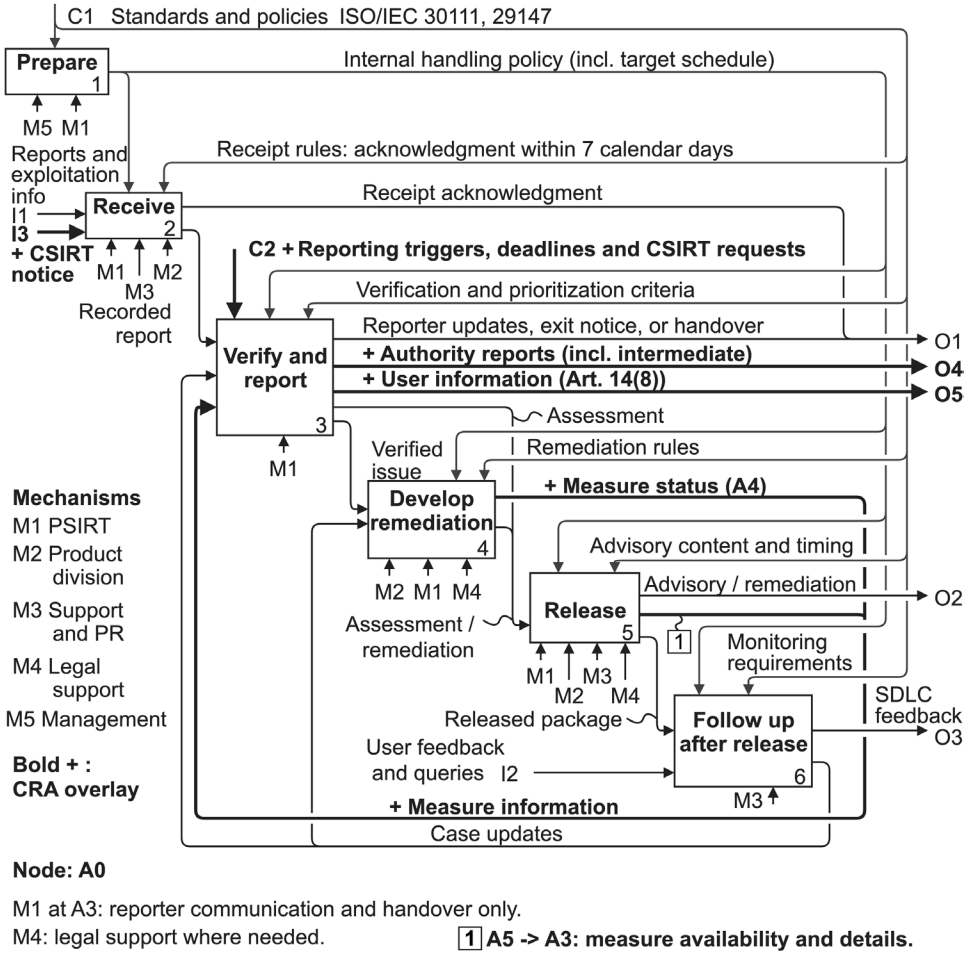


Figure 3: Vulnerability handling with CRA reporting.

Article 14(2) requires an early warning without undue delay and within 24 hours of awareness, and a vulnerability notification without undue delay and within 72 hours. The final report is due within 14 days after a corrective or mitigating measure becomes available. The notification and final report are required unless the relevant information has already been provided. The coordinating CSIRT may request an intermediate report on status updates (Article 14(6)). C2 carries these conditions to A3.

Information needs change as handling progresses. Early warnings may be due before remediation is complete; the 72-hour notification includes measure information as available, and the final report includes details of available measures (Article 14(2)(b), (c)(iii)). A4 therefore supplies measure status to A3, while A5 supplies availability and details. Final reporting does not require repeating A4 or A5 and may overlap follow-up at A6.

O4 reaches the coordinating CSIRT and the European Union Agency for Cybersecurity (ENISA) simultaneously through the single reporting platform (Articles 14(1), (7), 16(1)). Article 14(8) requires information for impacted users and, where appropriate, all users. Where necessary, it includes mitigating or corrective measures that users can deploy, using a structured, machine-readable format where appropriate. User information must be timely, although the provision sets no numerical deadline.

Authority reporting (O4) differs from public advisories at A5. A5 groups advisory publication and remediation release, which need not occur together (29147 5.6.6, 7.3). An advisory may contribute to O5 user information, but the model distinguishes these functions.

Reporting and User Information Responsibilities

ISO/IEC 30111 describes PSIRT communication with reporters and information sharing (6.5.3.3, 6.5.3.5). FIRST describes investigation and reproduction by PSIRTs or dedicated teams with support from other expertise (2020, pp. 40, 52). M1 at A3 represents reporter communication and handover coordination; it does not assign PSIRT authority over all CRA reporting decisions, approvals, and submissions.

The examined CRA provisions impose duties on manufacturers without naming the internal departments performing each task. Table 2 identifies the documentary and model basis for these tasks and the internal assignments that manufacturers must determine.

Table 2: Reporting and user information responsibilities.

Function	Documentary and Model Basis	Internal Assignment
Reportability	CRA 3(42), 14(1). Technical assessment: 30111 7.1.4.	Who assesses evidence and decides reportability?
Report preparation and updates	CRA 14(2), (6). Model: information from A2–A5 and other providers.	Who gathers information and prepares and updates reports?
Decision and approval authority	30111 6.4; examined CRA provisions do not specify internal approval routes.	Who decides to submit and, where needed, approves submission?
Authority submission	CRA 14(1), (7), 16(1).	Who submits through the single reporting platform?
User information	CRA 14(8); 29147 7.3.	Who prepares information and provides it to users?

ISO/IEC 30111 requires an internal policy defining handling responsibilities and recommends a role with decision authority (6.3, 6.4). IEC 62443-4-1 also requires the identification of responsible roles

for its processes (5.4.1). Manufacturers must build on these provisions to assign specific responsibilities and authority for reporting and user information.

DISCUSSION

The standards already address exploitation in prioritization and remediation, as well as advisories issued before a remediation is available (30111 7.1.4 e), 7.1.5; 29147 5.6.6, 7.3). Article 14 adds statutory notification conditions, recipients, and deadlines. Figure 3 shows that CRA reporting requires information produced by several activities at different times. In FIRST's distributed PSIRT model, triage and remediation staff do not report directly to PSIRT operations (2020, pp. 7–9). Such arrangements require clarity about who supplies information and who decides and submits reports. After awareness, holding a report until the investigation is complete may make the statutory deadlines harder to meet. Reporting therefore involves human factors concerns about information handovers and decision-making across teams, alongside technical work.

Public disclosure coordination and CRA authority reporting follow different conditions. Reporting may be due while an advisory remains under embargo (29147 5.6.8). Manufacturers must distinguish between submission to authorities and public release, coordinating these decisions with information sensitivity and the duty to inform users (CRA Article 14(2) (b), (8)).

Awareness, which starts the reporting deadlines, also involves internal judgment and communication. The Commission's non-binding guidance calls for immediate initial assessment of suspicious events and describes awareness as reaching a reasonable degree of certainty of active exploitation after that assessment (2026, paragraphs 213–215). At A1, manufacturers can identify who assesses the evidence, how the findings are escalated, and who may submit reports. Recording the evidence and assessment times supports subsequent review of investigation and handovers. Establishing these responsibilities and information routes is an organizational task for integrating CRA reporting into existing handling.

Limitations

This study covers selected provisions on reporting actively exploited vulnerabilities, not the CRA's full vulnerability handling obligations. The diagrams show major information dependencies but omit some details, including the providers of individual report fields. Placing reporting at A3 is an analytical choice and does not prescribe an organizational structure.

The interpretations and mapping have not been independently coded or evaluated in manufacturer organizations. The results identify information dependencies and assignment questions but do not establish suitable staffing, operational ability to meet deadlines, or the extent of handover risks.

CONCLUSION

By mapping CRA Article 14 onto existing vulnerability handling, we identify reporting dependencies and the responsibilities manufacturers must assign internally. Authority reports may be required while investigation, remediation development, and disclosure coordination continue; later reports need updates from development and release. The documents describe technical and communication roles, while manufacturers must assign responsibility for assessing reportability, preparing and updating reports, authorizing and submitting them, and informing users. Further work should examine how organizations connect external evidence, internal judgments, authority reporting, and user information, and evaluate whether these arrangements work in practice.

ACKNOWLEDGMENT

This work was partially supported by the Industrial Cyber Security Center of Excellence (ICSCoE), Innovation Platform Agency, Japan. Any remaining errors are the authors' own.

REFERENCES

BSI (2025). Draft BS EN 40000-1-3. Cybersecurity requirements for products with digital elements – Part 1-3: Vulnerability Handling. Draft for comment 25/30550631 DC, 12 December 2025. London: British Standards Institution.

CERT/CC (n.d.). Vulnerability Disclosure Policy. Carnegie Mellon University. https://certcc.github.io/certcc_disclosure_policy/ (accessed 15 October 2026).

Davaadorj, N. (2018). Fundamental Study on Security Management Framework for Critical Infrastructures based on Safety-II (in Japanese). Doctoral dissertation. Nagoya: Nagoya Institute of Technology.

European Commission (2026). Commission guidance on the application of Regulation (EU) 2024/2847 (Cyber Resilience Act). Annex to C(2026) 5252 final, 27 July 2026. Brussels: European Commission.

European Parliament and Council (2024). Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements. Official Journal of the European Union, 20 November 2024. https://data.europa.eu/eli/reg/2024/2847/oj

FIRST (2020). Product Security Incident Response Team (PSIRT) Services Framework. Version 1.1. 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: IEC.

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

ISO/IEC (2019). ISO/IEC 30111:2019. Information technology—Security techniques—Vulnerability handling processes. Geneva: ISO.

Iwasaki, Y. (2021). A Study on Management Framework based on Risk Appetite (in Japanese). Doctoral dissertation. Nagoya: Nagoya Institute of Technology.

NIST (1993). Integration Definition for Function Modeling (IDEF0). Federal Information Processing Standards Publication 183. Gaithersburg, MD: National Institute of Standards and Technology.

Ruohonen, J. and Timmers, P. (2025). Vulnerability Coordination under the Cyber Resilience Act. Applied Cybersecurity & Internet Governance, 4(1). https://doi.org/10.60097/ACIG/213350

Tahara, J. and Watanabe, K. (2025). Coordinating Asset Owner and PSIRT for CRA Vulnerability Recognition: Evidence-Based Mechanisms From Coordination Theory. Applied Human Factors and Ergonomics, 199, pp. 2291–2301. https://doi.org/10.54941/ahfe1007041

Tahara, J., Watanabe, K., Koshijima, I. and Oka, R. (2025). Resolving Conflicts Between PSIRT and Safety Teams: A Collaborative Approach. Human Factors in Cybersecurity, 168, pp. 70–81. https://doi.org/10.54941/ahfe1006144