Comparative Analysis of Methodological Approaches to Cyber Resilience Assessment in International Standards, Regulations, and Industry Frameworks

Serhii Honchar[1,*], Olena Ogir[1], Volodymyr Artemchuk[1,2,3]

[1] G.E. Pukhov Institute for Modelling in Energy Engineering of the National Academy of Sciences of Ukraine, 15, General Naumov Str., 03164 Kyiv, Ukraine

[2] Center for Information-Analytical and Technical Support of Nuclear Power Facilities Monitoring of the NAS of Ukraine, 34-A Akademika Palladina Ave., 03142 Kyiv, Ukraine

[3] Department of Computer Science, Kyiv National Economic University named after Vadym Hetman, 54/1 Beresteysky Prospect, 03057 Kyiv, Ukraine

Abstract

This paper presents a comparative analysis of selected international standards, regulatory acts, and industry frameworks for cyber resilience assessment. Given the limitations of traditional perimeter-focused cybersecurity, maintaining the resilience of critical information infrastructure (CII) under conditions of successful compromise has become increasingly important. The study compares nine selected standards, regulations, and frameworks - including NIST SP 800-160, DORA, and CAF - and applies an AHP-informed multi-criteria scoring procedure across criteria such as technical depth, adaptability, economic efficiency, and regulatory significance. The findings provide a structured classification to support national resilience strategies and guide sector-specific framework selection.

Keywords

Cyber resilience, critical information infrastructure, resilience frameworks, cyber resilience assessment 1

1. Introduction

In the current threat landscape, it is impossible to guarantee the complete security of any information system, including critical information infrastructure (CII), against cyberattacks [1]. Whereas the primary objective of cybersecurity has traditionally been prevention, cyber resilience emphasizes recovery, adaptation, and continuity of critical functions. As noted in [2], cybersecurity focuses on hardening a system to avoid functional degradation, while cyber resilience focuses on restoring and adapting functionality after disruption. Consequently, minimizing recovery time and protecting vital components become central tasks. Cyber resilience of CII can be understood as the ability to maintain reliable operation and provide essential services under cyber-threat conditions [3].

Therefore, the aim of this paper is to compare selected international standards, regulatory acts, and industry frameworks for cyber resilience assessment and to identify their applicability to CII entities. The study focuses on three resilience domains—asset management, detection and response, and recovery/regeneration—and four assessment criteria: technical depth, adaptability, economic efficiency, and regulatory significance.

2. Relevance of the Research

According to CERT-UA [4] and public reports based on NSDC data [5], approximately 5,927 cyber incidents were processed by CERT-UA in Ukraine in 2025, which is 37.4% more than in 2024 (4,315 incidents). In comparison, 1,350 attacks were recorded in 2021. Local government authorities (35.7% of all attacks), the energy sector, and the defense sector faced the greatest pressure.

[1]RS-2026: Resilient Systems: Secure Digital Technologies and Critical Infrastructure, June 30, 2026, Drohobych, Ukraine

* Corresponding author.

sfgonchar@gmail.com (S. Honchar), olena.ogir@pimee.ua (O. Ogir), volodymyr.artemchuk@pimee.ua (V. Artemchuk)

0000-0002-9978-8998 (S. Honchar), 0000-0001-9623-399X (O. Ogir), 0000-0001-8819-4564 (V. Artemchuk)

According to the Check Point Research report [6], the number of weekly attacks per organization worldwide increased by 30% in Q2 2024 compared with Q2 2023, reaching an average of 1,636 attacks per organization per week. The government and military sectors consistently rank among the top three most targeted industries.

In 2024–2025, public threat reports indicate that critical infrastructure remains a major target of sophisticated cyberattacks, including energy, transport, and water supply systems. The use of generative AI (GenAI) has further enabled attackers to scale phishing and identity-fraud operations and to automate vulnerability discovery, highlighting the limitations of traditional defense methods [7, 8].

3. Statement of the Problem

These statistics indicate that the classical cybersecurity concept, focused primarily on intrusion prevention, is insufficient for the current threat landscape. It is increasingly complemented by the cyber resilience concept, which emphasizes the ability of a system to maintain critical functions even in the event of a successful compromise.

The practical problem is not only the growing number and sophistication of attacks, but also the absence of a sufficiently transparent and sector-sensitive approach to selecting an appropriate resilience-assessment framework for different sectors of critical information infrastructure. This makes a comparative analysis of modern standards, regulations, and frameworks crucial for developing national resilience strategies and sector-specific assessment practices.

4. Methodology

The study applies a comparative content analysis of selected international standards, regulations, and frameworks, followed by an AHP-informed multi-criteria prioritization procedure. The procedure included three steps: (1) selecting documents according to relevance, sectoral representativeness, and methodological diversity; (2) assessing each document across three resilience domains (asset management, detection and response, and recovery/regeneration); and (3) comparing the frameworks using four criteria (technical depth, adaptability, economic efficiency, and regulatory significance). These criteria reflect both technical and institutional aspects of cyber resilience assessment.

The resulting scores were normalized on a scale from 0 to 1, where 1 indicates the strongest alignment with the criterion. In this short conference paper, pairwise-comparison matrices and consistency-ratio calculations are not reported; therefore, the procedure is treated as an AHP-informed multi-criteria scoring approach rather than as a full AHP implementation.

5. Research Results

Nine documents (international standards, regulatory acts, and industry frameworks) were selected for the analysis. They are among the most influential and widely used sources in the field of system cyber resilience assessment. The selection was based on the following criteria:

• Relevance and Status: Priority was given to active international standards, national/institutional guidance, and EU legislative acts that came into force, were updated, or gained practical relevance during 2022–2024.

• Sectoral Representativeness: The selected approaches cover various sectors, ranging from general-purpose frameworks to sector-specific instruments: financial (DORA), energy and CII-oriented assessment (CAF), and digital-product manufacturing/software development (CRA).

• Methodological Diversity: The sample includes quantitative indicators (CRI), qualitative maturity models (CERT-RMM, CRR), and engineering-driven approaches (NIST, MITRE).

The analysis allowed these documents to be classified as follows:

a) International Standards and National/Institutional Guidance:

• NIST SP 800-160 Vol. 2 (Developing Cyber-Resilient Systems): A primary guidance document describing an engineering approach to building and assessing cyber-resilient systems. It proposes 14 techniques (e.g., adaptive response, segmentation, redundancy) to achieve resilience goals;

• ISO/IEC 27001 and ISO 22301: While these standards focus on information security management and business continuity, their combination is frequently used as a baseline for assessing resilience to cyber incidents;

b) Methodological and Sectoral Frameworks:

• MITRE Cyber Resiliency Engineering Framework (CREF): The framework upon which the NIST SP 800-160 standard is based. It includes a matrix linking goals, objectives, and specific engineering practices;

• Cyber Assessment Framework (CAF): Developed by the UK National Cyber Security Centre (NCSC), this framework provides specific indicators of good practice for critical infrastructure;

• CERT Resilience Management Model (CERT-RMM): A comprehensive maturity model for managing operational resilience, covering security processes, business continuity, and IT operations;

• Cyber Risk Index (CRI): A quantitative indicator intended to estimate the gap between organizational preparedness and the threat landscape;

• Cyber Resilience Review (CRR): A methodology by CISA (based on CERT-RMM) for assessing organizational capabilities across 10 domains, including asset management, training, and incident response;

c) Regulatory and Legislative Acts:

• DORA (Digital Operational Resilience Act): A European regulation for the financial sector that establishes clear requirements and testing methods for digital resilience (e.g., TLPT — Threat-Led Penetration Testing);

• Cyber Resilience Act (CRA): EU legislation introducing standardized cybersecurity and resilience requirements for digital products throughout their entire lifecycle.

A comparative analysis of the aforementioned standards, regulations, and frameworks, based on critical criteria and key resilience domains (stages), is presented in Table 1.

Table 1
Comparative Characteristics of Standards, Regulations, and Frameworks

Document Name	Object of Assessment	Primary Methodology	Asset Management	Detection and Response	Recovery and Regeneration

NIST SP 800-160 Vol. 2	IT System / Architecture	14 engineering techniques (e.g., segmentation, adaptability, redundancy)	High: focus on dynamic configuration changes	High/Technical: adaptive response, deception, segmentation, and other cyber-resiliency techniques	Maximum: regeneration, non-persistence, and architectural recovery mechanisms
ISO/IEC 27001 & 22301	ISMS / Business processes	PDCA cycle (Plan-Do-Check-Act) and audit	High/Basic: ISMS asset inventory and control requirements, but limited resilience-specific asset dynamics	Medium/Process-based: incident management and logging	High: separate 22301 standard for Business Continuity
MITRE CREF	Design processes	Relationship matrix: Goals – Objectives – Techniques	Medium: assets considered through mission criticality	High: linking techniques to specific attack types	Medium: focus on minimizing attack impact
Cyber Assessment Framework (CAF)	Critical infrastructure	14 principles and Indicators of Good Practice (IGP)	High: specific "Asset Management" principle for CII	Maximum: real-time anomaly monitoring and outcome-based response indicators	High: emphasis on "Lessons Learned"
CERT-RMM	Organization (as a whole)	26 domains, maturity levels	Maximum: 4 domains dedicated to asset management	High/Process-based: detailed procedures for incident management	Medium: recovery through process maturity levels
Cyber Resilience Review (CRR)	Capabilities	10 domains (based on CERT-RMM)	Basic: identification of critical services	Medium: simplified incident questionnaires	Basic: verification of recovery plans existence
Cyber Risk Index (CRI)	Risk landscape	Calculation of gap between threats and readiness	Medium/Analytical: vulnerability assessment of critical assets	Low/Statistical: assessment of detection readiness	Low: evaluates only loss probability
DORA (EU Act)	Financial sector and providers	Mandatory testing and reporting	Strict: register of all IT assets and provider links	Maximum: mandatory threat-led penetration testing	High: strict timeframes for service recovery
Cyber Resilience Act (CRA)	Digital goods (IoT, software)	Product lifecycle requirements	Medium/Product-based: inventory of software vulnerabilities	Medium/Technical: vulnerability reporting and security-support obligations	Medium: security support throughout product life

The scoring was based on content analysis of each document according to predefined qualitative descriptors. When composite labels are used in Table 1, the first term indicates the coverage level, while the second term clarifies the dominant implementation orientation.

• "Maximum / Strict": the document contains detailed technical requirements, clear time-bound KPIs (e.g., as in DORA), or step-by-step engineering instructions for process automation;

• "High": a separate, extensive section or domain is dedicated to the issue, featuring an outcome-based description;

• "Medium": the issue is mentioned as part of a general process, but without detailing its implementation methods;

• "Basic / Low": the issue is addressed declaratively, or only the mere existence of a corresponding policy is evaluated without verifying its effectiveness.

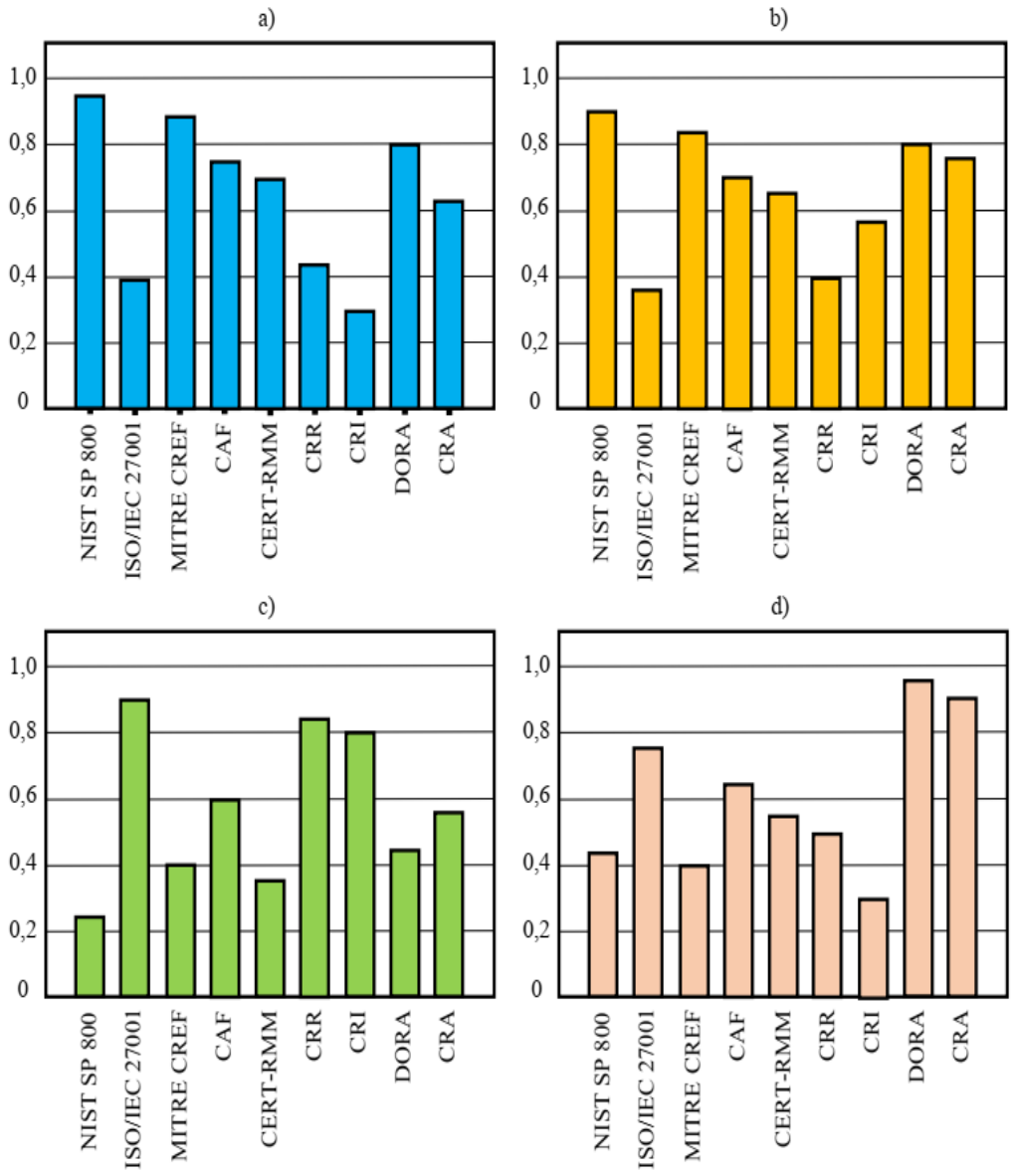

Figure 1: Normalized priority scores of cyber resilience frameworks according to individual AHP-informed criteria: a) technical depth (c1); b) adaptability (c2); c) economic efficiency (c3); d) regulatory significance (c4).

Figure 1 presents normalized priority scores for the analyzed frameworks according to each criterion. NIST SP 800-160 and MITRE CREF receive the highest scores in technical depth due to their engineering-oriented structure, while DORA and CRA show higher regulatory significance

because of their binding legal status in the European context. CAF demonstrates strong applicability to CII operators because it links assessment to concrete outcomes and indicators of good practice.

The results indicate that no single framework dominates across all criteria. Therefore, framework selection should depend on the sector, regulatory context, organizational maturity, and intended depth of assessment. CRI is more suitable as a risk-indicator tool than as a comprehensive resilience-assessment framework, whereas CERT-RMM and CRR are more relevant when organizational process maturity is the main assessment objective.

6. Conclusions

Based on the comparative analysis of nine selected international standards, regulations, and cyber resilience frameworks, CAF appears to be one of the most suitable frameworks for CII entities in the context of outcome-based cyber resilience assessment. DORA is particularly relevant for the financial sector because of its binding testing, reporting, and recovery requirements, whereas CRA is especially relevant for digital-product manufacturers and software developers because it introduces lifecycle-oriented cybersecurity obligations for digital products. NIST SP 800-160 and MITRE CREF demonstrate high technical maturity, but their implementation requires substantial engineering expertise and organizational resources.

The contribution of this paper is not the development of a new cyber resilience standard, but a structured comparative mapping of heterogeneous resilience-oriented instruments—international standards, regulatory acts, and methodological frameworks—within a unified assessment logic. In contrast to purely descriptive overviews, the paper combines domain-level comparison with an AHP-informed multi-criteria scoring procedure, allowing the suitability of different instruments to be interpreted in relation to CII needs, sectoral context, regulatory pressure, and implementation complexity.

The practical value of the proposed comparison lies in its use as an initial decision-support instrument for selecting cyber resilience assessment approaches. For CII operators, regulators, and policy planners, the comparison helps distinguish between technically deep engineering frameworks, legally binding sectoral regulations, maturity-oriented organizational models, and risk-indicator tools.

At the same time, the study is limited by the qualitative nature of the scoring procedure, the selection of nine documents, and the absence of fully reported expert pairwise-comparison matrices. Future work should include expert validation, consistency-ratio reporting, and sector-specific case studies for Ukrainian CII. Such validation would make it possible to move from a generalized comparative assessment toward operational recommendations for specific critical infrastructure sectors.

Acknowledgements

This research combines independently conducted work with selected activities carried out within a grant-supported research framework. The grant-supported part of the research was funded by the U.S. National Academy of Sciences (NAS) and the Office of Naval Research Global (ONRG) through the Science and Technology Center in Ukraine (STCU) under STCU contract number 7126, within the framework of the International Multilateral Partnerships for Resilient Education and Science System in Ukraine (IMPRESS-U).

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT (OpenAI) for translation support, grammar and spelling checks, paraphrasing, language improvement, proofreading, and editorial refinement. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] V. Mokhor, S. Honchar, A. Onyskova, Cybersecurity Risk Assessment of Information Systems of Critical Infrastructure Objects, in: Proceedings of the 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology, PIC S&T '20, IEEE Press, Kharkiv, Ukraine, 2020, pp. 19–22. doi:10.1109/PICST51311.2020.9467957.

[2] A. Kott, I. Linkov, To Improve Cyber Resilience, Measure It, Computer 54 (2021) 80–85. doi:10.1109/MC.2021.3049247.

[3] M. Komarov, S. Honchar, D. Dimitriieva, Doslidzhennia problemy kiberzhyvuchosti obiektiv krytychnoi informatsiinoi infrastruktury [Research on the problem of cyber survivability of critical information infrastructure objects], Nuclear and Radiation Safety 1 (2021) 59–66. doi:10.32918/nrs.2021.1(89).07.

[4] State Service of Special Communications and Information Protection of Ukraine, CERT-UA Processed Nearly 6,000 Cyber Incidents in 2025: Hostile Attack Volume Rose by 37%, 2026. URL: https://cip.gov.ua/en/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37.

[5] Vsviti, Record Number of Cyberattacks: NSDC Reported 6 Thousand Incidents in 2025, 2026. URL: https://vsviti.com.ua/news/175733.

[6] Check Point Research, Check Point Research Reports Highest Increase of Global Cyber Attacks Seen in Last Two Years: A 30% Increase in Q2 2024 Global Cyber Attacks, 2024. URL: https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/.

[7] U.S. House Committee on Homeland Security, Cyber Threat Snapshot, 2025. URL: https://homeland.house.gov/wp-content/uploads/2025/10/Cyber-Threat-Snapshot.pdf.

[8] AuthenticID, AuthenticID 2025 Annual Report Reveals Surge in Identity-Based Fraud Across Businesses, 2025. URL: https://www.authenticid.com/news_press/authenticid-annual-report-reveals-surge-in-identity-based-fraud-across-businesses/.