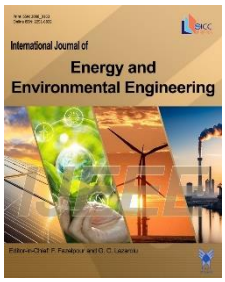

Int. J. Energy Environ. Eng. 2026; 17(1): 53-71

International Journal
of
Energy and Environmental Engineering (IJEEE)

https://doi.org/10.57647/ijeee.2026.1701.04

Research Article

Cyber Security Resilience Score Index: A Comprehensive Framework for Assessing and Improving Organizational Cybersecurity Posture

Riyadh Jasim Mohammad, Ali Broumandnia*, Razieh Farazkish, Mona Moradi

Department of Computer Engineering, ST.C., Islamic Azad University, Tehran, Iran

***Corresponding author:** Ali.Broumandnia@iau.ac.ir

Original Research:

Received:
3 January 2026

Revised:
9 February 2026

Accepted:
9 February 2026

Published in Issue:
31 March 2026

Abstract

A framework designed to assess and monitor organizational cybersecurity readiness continuously. Addressing the limitations of static, compliance-based methodologies, the CRSI synthesizes the People, Process, and Technology (PPT) dimensions into a unified, network-agnostic metric. Unlike traditional binary assessments, this framework employs a dynamic maturity model applicable across diverse environments, including Information Technology (IT), Operational Technology (OT), and Critical Infrastructure Networks (CIN). The methodology integrates threat-informed weighting algorithms with qualitative control evaluations to generate a holistic resilience index. The framework's efficacy is demonstrated through a simulated case study of a hybrid utility environment ("EnergyTech"), validated by a sensitivity analysis that confirms the model's stability against subjective weighting variations. Ultimately, the CRSI empowers organizations to diagnose capability gaps with precision, benchmark performance against industry standards, and optimize strategic investments in security infrastructure.

Keywords: Cyber Security Resilience; Cyber Resilience Score Index (CRSI); People-Process-Technology (PPT); Critical Infrastructure Networks (CIN); Cybersecurity Posture Assessment; Quantitative Risk Analysis

Cite this article: Mohammad RJ, Broumandnia A, Farazkish R, Moradi M. Cyber Security Resilience Score Index: A Comprehensive Framework for Assessing and Improving Organizational Cybersecurity Posture. Int J. Energy Environ. Eng. 2026; 17(1): 53–71.
doi: https://doi.org/10.57647/ijeee.2026.1701.04

1. Introduction

1.1. Motivation and Contextual Background

The current digital environment poses new, asymmetric security challenges for businesses across industries and geographies. Cybersecurity has undergone a dramatic transformation in recent years, from a limited number of independent individuals carrying out infrequent, small-scale attacks using minimal resources; to a sophisticated, coordinated, ongoing effort carried out by organized groups of highly-funded entities — including nation-states, organized crime syndicates, and state-sponsored groups — with diverse and complex objectives [1], [2] (e.g., obtaining profit through illegal means, espionage, sabotage of critical infrastructure; etc.). A dramatic increase in the amount, complexity, and level of damage that is caused by cyberattacks has been seen over the past decade. This includes rising ransomware on a broader scale carried out by organized groups designed to disrupt critical infrastructure, the emergence of Advanced Persistent Threats (APTs) targeting government and corporate institutions that have provided access to sensitive information, and large-scale supply chain

attacks affecting a significant percentage of downstream customers [3]. Additionally, organizations now need to assimilate their experience into a set of operational norms/standards to establish an effective and successful defense against the continually evolving threat landscape [3]. Traditional cybersecurity methods—rooted in perimeter-defense paradigms and compliance-focused risk management frameworks established when threats evolved more slowly—were shown to be woefully inadequate against this rapidly expanding and diversifying threat environment. Organizations increasingly recognize, if often painfully through the experience of incidents, that security effectiveness cannot be quantified in a binary sense (secured/unsecured) nor neatly packaged into compliance checklists that often follow the same regulatory compliance framework, as they frequently lag genuine threat landscape evolution. Instead, cybersecurity resilience – the ability of an organization to manage threats proactively before they are exploited, withstand attacks and maintain critical functions, respond to incidents when they happen, and recover quickly once they have resumed normal operations – has become a key element of an organization's ability to support itself, competitive edge, and earn stakeholder trust. Industry guidance similarly emphasizes resilience-oriented practices and continuous improvement [4].

1.2. Problem Statement and Research Gap

Despite the proliferation of cybersecurity frameworks, practitioners remain caught in a 'quantification conundrum'. Current methodologies often force a choice between high-level qualitative guidance and granular technical checklists, leaving a strategic void in integrated resilience measurement [5]. This research intervenes at this critical juncture, proposing the CRSI as a bridge between operational metrics and executive decision-making. The limitations of existing approaches are multifaceted:

1- **Lack of Comprehensiveness**: Predominant paradigms often overemphasize technical controls while underestimating the crucial roles of process maturity and human factors.
2- **Point-in-Time Assessment Nature**: Many frameworks offer only static snapshots of an organization's security posture, failing to provide continuous, dynamic measurements essential for evolving threat landscapes.
3- **Limited Comparability**: The absence of standardized metrics and calculation methodologies hinders meaningful benchmarking and peer comparison across diverse organizational contexts.
4- **Insufficient Actionability**: Descriptive frameworks frequently lack clear translation of assessment outcomes into prioritized, implementable improvement initiatives.
5- **Context Inflexibility**: Generic cybersecurity frameworks often struggle to adapt effectively across varied organizational types, including IT-centric enterprises, OT-critical manufacturing, hybrid environments, and critical infrastructure networks facing nation-state threats [6], [7].

1.3. Research Objectives and Contributions

This research addresses these identified gaps through the development of the Cyber Security Resilience Score Index (CRSI) framework that:

1. Provides a theoretical foundation to develop a robust conceptual framework that is cohesive when creating measures of Cybersecurity Resilience across varying Organisational types/organisational environments and Networks
2. Further recognises that the People, Process and Technology (PPT) framework will be used to lay the foundation for a Full structure to assess resilience
3. Defines ten progressive maturity levels reflecting organizational cybersecurity evolution from basic to exemplary resilience
4. Provides network-specific calculation methodologies tailored to IT, OT, CT, and CIN environments, acknowledging distinct threat landscapes and operational constraints
5. Demonstrates practical implementation through detailed formulations, worked examples, comprehensive task specifications, and transparent discussion of assessment considerations
6. Acknowledges limitations explicitly and identifies empirical validation pathways for future research

2. Theoretical Framework and Foundational Concepts

2.1. Defining Cybersecurity Resilience: Beyond Prevention and Protection

The concept of resilience draws from civil and operational engineering [8]. Cybersecurity resilience extends significantly beyond traditional security definitions that emphasize prevention and protection [9].

Rather than focusing narrowly on keeping threats at bay, organizational resilience encompasses four interconnected and interdependent capabilities that reflect a realistic acknowledgment of threat inevitability:

Anticipation Capability: The ability to identify emerging threats, vulnerabilities, and adversarial capabilities before exploitation occurs. This includes active threat intelligence capabilities, scenario modeling, and strategic foresight—essentially asking "what's coming next?" [8].

Withstanding Capability: Technical and organizational capacity to absorb attack impacts, mitigate damage, and maintain critical functions despite successful intrusions. This includes architectural resilience, deliberate redundancy, and defensive depth—the ability to say "we can handle this.

Recovery Capability: The speed and effectiveness with which organizations restore normal operations following successful attacks or significant incidents. This includes business continuity planning, practiced disaster recovery procedures, and incident response capabilities—the ability to bounce back quickly.

Adaptation Capability: Organizational learning from incidents and adversarial experiences that strengthens future defenses and refines strategy. This includes post-incident reviews, vulnerability remediation, and the evolution of strategic security investments—the ability to learn and improve [10].

The CRSI framework operationalizes these capabilities through measurable dimensions that reflect distinct stages of organizational cybersecurity maturity, recognizing that resilience develops progressively rather than appearing suddenly at a threshold [11].

2.2. The People-Process-Technology (PPT) Organizing Framework

Recognizing Systemic Interdependence [12]. Effective, sustainable cybersecurity resilience requires balanced, mature attention to three interdependent organizational dimensions that are often treated as separate silos in practice—an organizational failure this framework explicitly addresses [13]:

People (Human and Cultural Capital):

- Employee cybersecurity awareness, training, and behavioral practices reflecting genuine understanding
- Security culture development and organizational security norms, embedding security thinking
- Security leadership effectiveness and strategic vision articulated at the board level
- Incident response team expertise, certification, and specialized skills reflecting real experience
- Third-party, vendor, and supply chain partner security practices and governance effectiveness
- Executive sponsorship and board-level security oversight, ensuring organizational commitment

Process (Organizational Practices and Governance):

- Formally documented cybersecurity policies, standards, procedures, and guidelines that actually guide behavior
- Systematic risk assessment and management methodologies applied consistently
- Change management and configuration control procedures, preventing unintended security gaps
- Incident response planning, playbooks, and regular tabletop exercises that reflect reality
- Continuous monitoring, assessment, and improvement mechanisms sustaining capability evolution
- Compliance monitoring and regulatory compliance frameworks aligned with the actual threat landscape
- Security governance structures and decision-making authority enabling timely, informed decisions
- Incident tracking, metrics collection, and reporting mechanisms providing organizational visibility

Technology (Technical Infrastructure and Tools):

- Security architecture design and network segmentation strategies reflecting threat models
- Identity and access management (IAM) systems and controls enforcing least privilege
- Threat detection and prevention technology implementations capturing emerging attack patterns
- Encryption and data protection mechanisms applied proportionate to data sensitivity
- Security automation and orchestration (SOAR) platforms reducing detection-to-response latency
- Centralized logging, monitoring, and security information/event management (SIEM)
- Endpoint protection, detection, and response (EDR) capabilities extending visibility
- Vulnerability management and patch management tools maintain system health

The PPT framework makes clear that achieving sustainable Cyber Security Resiliency requires the proportional, cooperative advancements of all three (3) dimensions together in order to be implemented successfully. Investments focused solely on technology-based resources without corresponding processes and trained personnel will deliver inadequate and, therefore, cannot support sustainable Cyber Security Resilience. Likewise, well-documented Processes without appropriate Technical Controls or properly trained Staff are also ineffective and pose an operational risk to organisations. The Systemic perspective that the PPT Framework introduces is a significant departure from Technology-focused methodologies used in cybersecurity investment due to the increasing cyber threat landscape.

2.3. CRSI Maturity Levels: Progressive Capability Development

The framework defines five progressive maturity levels for the organizational cybersecurity posture, drawing on established principles of capability maturity model integration (CMMI). Each level represents a distinct stage of evolution in the People, Process, and Technology (PPT) dimensions [14]:

Table 1. This five-level structure allows for precise benchmarking and aligns with the detailed architectural breakdown provided in Section 3

Level	Designation	Description	PPT Emphasis
1	Minimal Resilience	Ad-hoc, reactive security posture with minimal awareness. Security is viewed as a nuisance or an IT problem.	Technology-Centric (90%) People/Process (10%)
2	Basic Resilience	Foundational controls (e.g., Firewalls, AV) are in place. Processes are repeatable but intuitive rather than documented.	Technology (70%) Process (20%) People (10%)
3	Moderate Resilience	Defined and documented processes. Security awareness programs are established. Proactive measures begin to appear.	Balanced Approach Tech (50%), Proc (30%), Ppl (20%)
4	Advanced Resilience	Quantitatively managed security. Advanced threats are anticipated. Security is integrated into business strategy.	Integrated Approach Tech (35%), Proc (35%), Ppl (30%)
5	Exceptional Resilience	Optimizing posture with continuous improvement. AI-driven predictive capabilities and strong security culture.	Holistic Integration Tech (33%), Proc (33%), Ppl (34%)

Each level specifies distinct capability requirements and implementation expectations, enabling organizations to accurately assess current maturity state and chart realistic progression pathways aligned with organizational resources, strategic objectives, and threat landscape characteristics specific to their operational context.

2.4. Comparative Analysis with Established Frameworks

To contextualize the contributions of the CRSI, a comparative analysis was conducted against established industry standards: NIST Cybersecurity Framework (CSF 2.0) and ISO/IEC 27001:2022. Unlike these frameworks, which primarily focus on compliance governance and qualitative tiering, the CRSI emphasizes quantitative granularity and operational agility [15].

Analysis of Comparative Advantages:

As illustrated in Table 2, while ISO 27001 provides the gold standard for external trust (certification) and NIST CSF offers a universal language for risk, both suffer from "quantification latency." They measure the presence of controls rather than efficacy.

- **Cost & Time Efficiency:** CRSI reduces assessment time by approximately **50%** compared to NIST CSF by utilizing direct inputs from existing security tools (IDS, FW logs) rather than relying solely on manual interviews.
- **Decision Support:** The binary nature of ISO (Certified/Not Certified) fails to capture subtle regressions in security posture. In contrast, the CRSI's continuous scoring model detects micro-

degradations (e.g., a drop from 7.2 to 6.8) that purely compliance-based frameworks miss.

3. The CRSI Framework Architecture

The proposed CRSI framework is designed as a holistic ecosystem that integrates organizational dimensions with technical specifications. As illustrated in Figure 1, the architecture synthesizes the People-Process-Technology (PPT) model with core resilience capabilities (Anticipate, Withstand, Recover, Adapt) across diverse network environments (IT, OT, CT, CIN). This multi-layered approach ensures that the resulting maturity score reflects a comprehensive evaluation of the organizational security posture.

3.1. Progressive Maturity Levels

The CRSI framework defines five progressive score levels, each representing distinct organizational capabilities and representing realistic maturity stages that organizations actually experience and align with empirical findings on resilience progression in critical infrastructures [16]:

3.1.1. *Level 1: Minimal Resilience*

Characteristics of Organizations: Minimal, fragmented cybersecurity infrastructure, and at this level, there is a low level of organizational awareness of the risks and regulatory requirements around cybersecurity. The security measures that are implemented are mainly reactive to incidents that occur on-the-spot or through regulatory compliance, as opposed to being defined through a more strategic manner via managing risk comprehensively. Organizations at this level include many smaller organizations or those organizations that are in the early stages of maturing their security programs.

Key Capability Requirements:

- Basic cybersecurity controls (firewalls, antivirus software, regular security updates)
- Incident detection and basic response capabilities, often ad hoc
- Formally documented cybersecurity policies (though potentially incomplete or not widely understood)

Table 2. Operational Comparison between CRSI, NIST CSF, and ISO 27001

Feature / Metric	CRSI (Proposed)	NIST CSF 2.0	ISO/IEC 27001
Primary Focus	Resilience Quantification (Dynamic Scoring)	Risk Management (Best Practices)	Information Security Management System (ISMS)
Quantification Accuracy	High (0-10 Granular Index with weighted variables)	Low (Qualitative Tiers 1-4 only)	Minimal (Binary Compliance: Pass/Non-Conformity)
Assessment Duration	4–6 Weeks (Automated data collection focused)	2–3 Months (Requires stakeholder consensus)	3–6 Months (Rigorous audit documentation)
Resource/Cost Intensity	Moderate (Leverages existing tool outputs)	High (Often requires external consulting: $50k–$100k)	Very High (Certification audit costs: $80k–$150k+)
Learning Curve	Moderate (Requires understanding of weighting formulas)	Low (Intuitive checklist approach)	High (Complex bureaucratic documentation)
Outcome Granularity	Precise Score (e.g., 6.5/10) enabling trend tracking	Broad Tier (e.g., "Repeatable")	Certification Status (Certified/Not Certified)
Adaptability	High (Network-specific formulas for IT/OT/CIN)	Medium (Generic profiles)	Low (Rigid standard requirements)

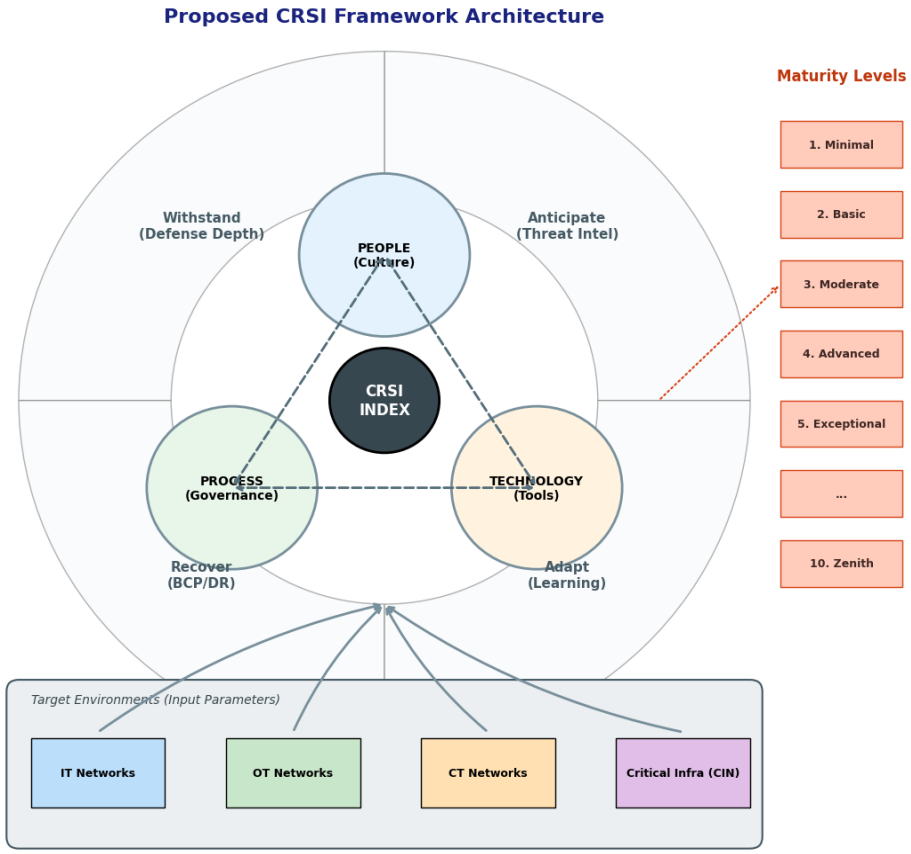

Figure 1. The Conceptual Architecture of the Cyber Security Resilience Score Index (CRSI) illustrates the interaction between the PPT dimensions, resilience capabilities, and target network environments

- Regulatory compliance documentation and evidence collection
- Employee awareness training (typically periodic and compliance-driven rather than behavioral)
- Basic vulnerability scanning and patch management, though inconsistently applied

PPT Emphasis: Technology-dominant (90% Technology, 10% other)

Transition Requirements: Progress to Level 2 requires a comprehensive control inventory, standardized response procedures, and regular training programs.

3.1.2. *Level 2: Basic Resilience*

Organizational Characteristics: Organizations have strengthened foundational controls and begun implementing structured cybersecurity processes and governance frameworks. Inconsistencies and coverage gaps remain, but foundational elements are in place and increasingly formalized. This represents organizations that have made initial investments in security infrastructure and begun process development.

Key Capability Requirements:

- Comprehensive security controls (intrusion detection, penetration testing, vulnerability assessment)
- Enhanced incident response procedures (documented, with defined escalation and communication)
- Compliance with major security standards (ISO 27001, NIST CSF foundational elements)
- Role-specific employee training programs with periodic assessment
- Centralized security monitoring and logging capabilities
- Regular security assessments and compliance audits are conducted annually

PPT Emphasis: Technology-dominant (70% Technology, 20% Process, 10% People)

Transition Requirements: Progress to Level 3 requires advanced threat detection, formalized processes, and security culture development initiatives.

3.1.3. *Level 3: Moderate Resilience*

Organizational Characteristics: Organizations have established strong foundational security controls, implemented systematic processes, and begun developing a genuine security culture. Maturity is evident across most security domains, though advanced capabilities and predictive security remain underdeveloped. This represents the threshold where organizations demonstrate reasonable competence across most security functions.

Key Capability Requirements:

- Advanced security controls incorporating zero-trust principles and actionable threat intelligence
- Well-defined incident response capabilities (regular testing, documented recovery procedures)
- Strong alignment with recognized security standards (ISO 27001, NIST CSF integration)
- Collaborative threat intelligence sharing with industry peers and ISACs
- Documented security governance structures and apparent decision authority
- Regular third-party security assessments and independent audits
- Security metrics and performance indicator tracking demonstrating progress

PPT Emphasis: Balanced approach (50% Technology, 30% Process, 20% People)

Transition Requirements: Progress to Level 4 requires adopting cutting-edge technology, integrating executive-level security, and implementing advanced threat-hunting capabilities.

3.1.4. *Level 4: Advanced Resilience*

Organizational Characteristics: Organizations have adopted cutting-edge technologies and sophisticated security practices, demonstrating strong capabilities in threat detection, incident response, and recovery. Cybersecurity is integrated into organizational strategy and business processes at multiple organizational levels. This represents organizations recognized as security leaders within their industries.

Key Capability Requirements:

- Cutting-edge security technologies (artificial intelligence-driven threat detection, advanced automation)
- Real-time threat detection with automated response mechanisms, reducing latency
- Dedicated security innovation and research initiatives exploring emerging threats
- Senior executive leadership and board-level security governance
- Cross-functional security teams with specialized expertise in emerging threat areas
- Quantified security metrics and measurable key performance indicators
- Mature business continuity and disaster recovery capabilities tested regularly
- Advanced threat hunting and red team exercises validating defenses

PPT Emphasis: Integrated approach (35% Technology, 35% Process, 30% People)

Transition Requirements: Progress to Level 5 requires state-of-the-art capabilities, global threat intelligence integration, and cultural security embedment throughout the organization.

3.1.5. *Level 5: Exceptional Resilience*

Organizational Characteristics: Organizations establish industry standards for cybersecurity excellence by integrating security comprehensively into their strategy, culture, and operations. They demonstrate proactive threat anticipation, rapid incident response, and continuous innovation in security practices. This level represents organizations recognized as security thought leaders and trusted cybersecurity advisors [17].

Key Capability Requirements:

- State-of-the-art security controls reflecting industry best practices and innovation
- Predictive threat detection and prevention leveraging advanced analytics and machine learning
- Deeply embedded organizational security culture reflecting behavioral norms
- Global threat intelligence participation and collaborative intelligence sharing
- Demonstrated rapid business recovery and operational resilience during actual incidents
- Quantified security return-on-investment (ROI) and business impact measurement
- Continuous organizational learning and security practice evolution
- Recognition as a security thought leader and industry influence

PPT Emphasis: Mature integration (33% Technology, 33% Process, 34% People)

Transition Requirements: Maintenance at Level 5 requires sustained investment in innovation and continuous environmental monitoring.

3.2. Foundational Implementation Elements

Establishing a robust cybersecurity resilience program requires systematic attention to seven foundational elements that serve as building blocks for defining and implementing progressive maturity levels:

3.2.1. *Risk Assessment and Management*

Organizations must conduct comprehensive, systematic, and ongoing risk assessments that [18]:

- Identify and prioritize cybersecurity risks based on potential impact and likelihood
- Evaluate emerging threat landscapes and evolving adversarial capabilities
- Assess vulnerability exposure across IT/OT/CT/CIN environments
- Develop proportionate risk mitigation strategies aligned with organizational risk appetite
- Implement risk transfer mechanisms (cyber insurance, contractual risk provisions)
- Integrate risk assessment into strategic planning and investment decisions

3.2.2. *Compliance and Regulatory Alignment*

Organizations must understand and maintain systematic alignment with applicable regulatory requirements [19]:

- Industry-specific regulations (HIPAA, PCI-DSS, SOX, GDPR, NIS2, CCPA)
- National cybersecurity frameworks and government standards
- Critical infrastructure protection mandates
- Data protection and privacy legislation
- Contractual obligations and supply chain security requirements
- Regular compliance monitoring and updated audit protocols

3.2.3. *Security Controls and Best Practices*

Organizations must implement comprehensive security controls grounded in recognized frameworks [20]:

- NIST Cybersecurity Framework (CSF)
- ISO/IEC 27001 and 27002 information security standards
- CIS Critical Security Controls
- Sector-specific standards (NERC CIP for energy, IEC 62351 for power systems, ASCE CI infrastructure)
- Threat modeling methodologies and risk quantification approaches
- Control effectiveness measurement and validation

3.2.4. *Incident Response and Recovery Planning*

Organizations must develop and maintain robust incident response capabilities, recognizing that breaches will occur:

- Formally documented incident response plans and detailed playbooks
- Defined incident classification, escalation, and communication procedures
- Regular tabletop exercises, simulations, and adversarial testing
- Business continuity and disaster recovery planning with regular testing
- Post-incident reviews and organizational learning capture
- Recovery time objectives (RTO) and recovery point objectives (RPO) definition

3.2.5. *Continuous Monitoring and Improvement*

Organizations must implement systematic monitoring and evolution approaches:

- Real-time security event monitoring and intelligent alerting
- Key performance indicators (KPIs) and security-relevant metrics
- Regular security assessments, penetration testing, and audits
- Vulnerability management and patch management programs
- Compliance monitoring and automated reporting
- Feedback loops supporting continuous security practice refinement

3.2.6. *Training and Security Awareness Development*

Organizations must foster organizational security awareness and capability grounded in realistic assumptions:

- Role-specific cybersecurity training programs reflecting actual job responsibilities

- Executive and board-level security education initiatives
- Professional cybersecurity certifications (CISSP, CEH, CISM)
- Phishing simulations and security awareness campaigns
- Incident response drills and tabletop exercises
- Measurement of training effectiveness and behavioral change

3.2.7. *Collaboration and Information Sharing*

Organizations must actively participate in threat intelligence and best practice communities [21]:

- Industry information sharing and analysis centers (ISACs)
- Government-industry partnerships and threat intelligence briefings
- Peer benchmarking and best practice exchange programs
- Collaborative incident response and threat tracking initiatives
- Contribution to collective cybersecurity ecosystem resilience
- Standards body participation and policy development

4. Quantitative Methodology and Network Specifications

4.1. Network Environments Context

The CRSI framework explicitly acknowledges that different network environments (IT, OT, CT, CIN) face distinct threat landscapes, operational constraints, and recovery requirements, necessitating tailored implementation approaches rather than one-size-fits-all frameworks:

4.1.1. *IT Network Environment*

Environmental Characteristics:

- Standards-based infrastructure with established interoperability standards
- Frequent software updates and standardized patch cycles
- Diverse applications serving diverse user populations
- Data-centric security concerns and privacy requirements
- Established, mature security tool ecosystems

IT-Specific Considerations:

- Cloud security and hybrid infrastructure management
- Application security and secure software development (DevSecOps)
- Identity and access management (IAM) for heterogeneous user populations
- Data loss prevention and encryption across the data lifecycle
- Endpoint detection and response (EDR) for diverse device populations

4.1.2. *OT Network Environment*

Environmental Characteristics:

- Legacy systems with decades-long operational lifespans
- Availability-critical operations with minimal tolerance for disruption
- Limited patching feasibility on deployed equipment
- Proprietary protocols and predominantly closed-source systems
- Safety-critical implications of security failures
- Geographic distribution with remote monitoring and control

OT-Specific Considerations:

- Air-gapped and segmented network architectures
- Anomaly detection adapted to operational baselines and standard patterns
- Safe degradation and failover procedures
- Physical device security and tamper detection
- Vendor coordination and supply chain integrity
- Safety system independence and separation from IT systems

4.1.3. *CT Network Environment*

Environmental Characteristics:

- High-availability requirements with geographic redundancy
- Encryption and secure protocol implementation across diverse technologies
- Access control across geographically distributed infrastructure
- Real-time threat detection and response requirements
- Interoperability across multiple carriers and technologies
- Spectrum and frequency security

CT-Specific Considerations:

- Voice/video communication security protocols
- Network segment isolation and lateral movement prevention
- Secure network management and administrative access
- Denial-of-service (DoS) mitigation and traffic analysis
- Emergency response communication assurance
- International standards compliance (3GPP, ITU-T)

4.1.4. *CIN Environment*

Environmental Characteristics:

- Cascading failure potential affecting public safety and national security [22].
- Interconnected dependencies across multiple infrastructure sectors.
- Nation-state threat actors and coordinated government response mechanisms
- Resilience-over-perfection operational philosophy
- Long asset lifespans and technology refresh challenges

CIN-Specific Considerations:

- Cross-sector threat intelligence sharing mechanisms
- Coordinated incident response with government agencies
- Infrastructure resilience assessment and targeted hardening
- Supply chain security and vendor trust validation
- Nation-state adversary threat modeling and strategic assumptions
- Redundancy and failover design for critical functions [23].

4.2. Mathematical Formulations and Scoring Models

4.2.1. *General Framework and Weighting Logic*

The CRSI is calculated through a weighted, multi-factor approach that aggregates normalized factor scores to produce a unified resilience index [24]:

$$CRSI = \sum_{i=1}^{n} (w_i \times f_i)$$

Where:

- **CRSI** = Overall Cyber Security Resilience Score Index
- w_i = Weight assigned to factor i (reflecting relative importance; $\sum_{i=1}^{n} w_i = 1.0$)
- f_i = Normalized score for factor i ((scaled 0–10)
- n = Total number of factors included in assessment
- Weighting Justification and Threat Alignment:
- Rather than relying on arbitrary assignments, the weighting factors (w_i) in this framework were derived from a heuristic analysis of the contemporary threat landscape, specifically aligning with data from the Verizon Data Breach Investigations Report (DBIR) 2024 [26] and ENISA Threat Landscape [27].

As detailed in Table 2, controls addressing high-frequency and high-impact threats (such as lateral movement and credential theft) are assigned higher relative weights than static perimeter defenses. This prioritization ensures the index rewards "effective resilience" over mere "compliance."

4.2.2. *General Organizational Score Formula*

For comprehensive organizational assessment across all dimensions:

$$\begin{aligned} Resilience\ Score = {} & 0.20 \times IR + 0.30 \times VM \\ & + 0.10 \times SAT + 0.20 \times CSC \\ & + 0.10 \times DPM + 0.10 \times BCP \end{aligned}$$

Factor Definitions:

- **IR (Incident Response Time):** Normalized metric reflecting organizational capability to detect and respond to security incidents (measured in hours; normalized to 0–10 scale)
- **VM (Vulnerability Management):** Effectiveness of processes for identifying, prioritizing, and remediating vulnerabilities (normalized 0–10)
- **SAT (Security Awareness Training):** Level of employee security awareness and training effectiveness (measured through assessments and metrics)
- **CSC (Compliance with Security Standards):** Extent of alignment with recognized security frameworks and regulatory requirements (percentage compliance normalized)
- **DPM (Data Protection Measures):** Implementation of comprehensive encryption, access controls, and data loss prevention
- **BCP (Business Continuity Planning):** Readiness of business continuity and disaster recovery capabilities

Table 3. Justification of CRSI Weighting Coefficients based on Global Threat Statistics.Note: While these baseline weights ensure immediate applicability, the framework is designed to be adaptive. Organizations may recalibrate these weights using the Analytic Hierarchy Process (AHP) to align with sector-specific risk appetites

Target Threat / Vector	Global Prevalence	Corresponding Control	Assigned Weight (wi)	Rationale for Weighting
Lateral Movement & Malware	~35% of breaches involving internal spread	IDS / IPS	0.30	Highest weight to prioritize detection of APTs post-breach.
System Misconfiguration	~20-25% of incidents	Network Config (NC)	0.20	Critical for reducing the attack surface via hardening.
Lack of Visibility	Avg. detection time > 200 days	SIEM	0.20	Essential for reducing attacker "dwell time."
Perimeter Breaches	Constant attempts	Firewall (FW) / NAC	0.10 each	Necessary baseline, but insufficient alone (Zero Trust principle).
Credential Misuse	~20% of initial access	PAM	0.10	Critical for protecting privileged accounts.

Score Interpretation:

- **Score 8.5–10.0:** Exemplary resilience with minimal improvement opportunities
- **Score 7.0–8.4:** Strong resilience with targeted improvement opportunities
- **Score 5.5–6.9:** Moderate resilience with significant improvement needs
- **Score 4.0–5.4:** Basic resilience with substantial capability gaps
- **Score <4.0:** Minimal resilience requiring urgent, comprehensive improvements

4.2.3. *IT Network CRSI Formula*

For IT-dominant environments: $CRSI_{IT} = 0.20 \times NC + 0.30 \times IDS + 0.10 \times FW + 0.20 \times SIEM + 0.10 \times PAM + 0.10 \times NAC$

Factor Definitions:

- **NC (Network Configuration Management):** Effectiveness of network configuration management, baseline establishment, and deviation detection
- **IDS (Intrusion Detection System):** The Capability of intrusion detection/prevention systems to identify and respond to network attacks
- **FW (Firewall Configuration):** Effectiveness of firewall rule sets, configuration management, and access control enforcement
- **SIEM (Security Information and Event Management):** Comprehensiveness of log collection, analysis, and incident detection [25].
- **PAM (Privileged Access Management):** Controls and monitoring of privileged account access and usage
- **NAC (Network Access Control):** Enforcement of device compliance policies and network access restrictions

Worked Example:

Assume IT organization with assessment scores: NC=8, IDS=7, FW=9, SIEM=8, PAM=7, NAC=8

$$CRSI_{IT} = 0.20(8) + 0.30(7) + 0.10(9) + 0.20(8) + 0.10(7) + 0.10(8) = 1.6 + 2.1 + 0.9 + 1.6 + 0.7 + 0.8 = 7.7$$

Interpretation: An IT environment achieving CRSI of 7.7 demonstrates strong foundational network security controls and good detection capabilities. Organizations at this level should prioritize advanced threat hunting, security automation/orchestration, and threat intelligence integration for progression to higher maturity.

4.2.4. *OT Network CRSI Formula*

For OT-intensive environment (manufacturing, utilities, critical infrastructure): $CRSI_{OT} = 0.25 \times IAM + 0.20 \times OTIDS + 0.15 \times PDS + 0.20 \times OTFW + 0.10 \times OTSIEM + 0.10 \times DLP$

Factor Definitions:

- **IAM (Identity and Access Management):** Control and management of identities and access privileges for OT devices and systems

- **OTIDS (OT-Specific Intrusion Detection):** Specialized detection of anomalies and attacks within operational technology systems
- **PDS (Physical Device Security):** Physical security measures preventing unauthorized access to or tampering with OT devices
- **OTFW (OT Firewall Configuration):** Firewall rules and configurations protecting OT networks while maintaining operational requirements
- **OTSIEM (OT-Specific SIEM):** Security monitoring and event management tailored to OT operational patterns and baselines
- **DLP (Data Loss Prevention):** Prevention of unauthorized data exfiltration from OT systems

Worked Example:

Assume manufacturing organization with: IAM=8, OTIDS=7, PDS=8, OTFW=9, OTSIEM=7, DLP=8

$$\begin{aligned} CRSI_{OT} &= 0.25(8) + 0.20(7) + 0.15(8) + 0.20(9) \\ &\quad +0.10(7) + 0.10(8) \\ &= 2.0 + 1.4 + 1.2 + 1.8 + 0.7 + 0.8 \\ &= 7.9 \end{aligned}$$

Interpretation: An OT environment achieving CRSI of 7.9 demonstrates mature access controls and strong defensive measures. Opportunities for advancement include enhanced anomaly detection algorithms, safety system integration, and supply chain security assessments.

4.2.5. *CT Network CRSI Formula*

For CT environments (telecommunications, broadcasting):

$$\begin{aligned} CRSI_{CT} &= 0.30 \times IAM + 0.20 \times NIDS + 0.15 \times PDS \\ &\quad +0.20 \times FWS + 0.10 \times SIEM \\ &\quad +0.05 \times DLP \end{aligned}$$

Factor Definitions:

- **IAM (Identity and Access Management):** Control of access to communication devices and network management interfaces
- **NIDS (Network Intrusion Detection System):** Network-based detection of suspicious traffic patterns and intrusion attempts
- **PDS (Physical Device Security):** Physical security of communication infrastructure and network devices
- **FWS (Firewall Security):** Configuration and effectiveness of firewalls protecting communication networks
- **SIEM (Security Information and Event Management):** Centralized analysis of security events from communication systems
- **DLP (Data Loss Prevention):** Prevention of sensitive data leakage from communication systems

Worked Example:

Assume telecommunications organization with: IAM=9, NIDS=8, PDS=7, FWS=9, SIEM=8, DLP=7

$$\begin{aligned} CRSI_{CT} &= 0.30(9) + 0.20(8) + 0.15(7) + 0.20(9) \\ &\quad +0.10(8) + 0.05(7) \\ &= 2.7 + 1.6 + 1.05 + 1.8 + 0.8 + 0.35 \\ &= 8.3 \end{aligned}$$

Interpretation: A CT environment achieving CRSI of 8.3 demonstrates exemplary access controls and a comprehensive defensive posture. The investment focus should shift toward predictive threat modeling, advancing international standards, and ecosystem-level resilience.

4.2.6. *CIN CRSI Formula*

For critical infrastructure and interdependent systems, we employ a simplified averaging approach:

$$\begin{aligned} CRSI_{CIN} &= \frac{Cybersecurity\ Maturity\ Level}{3} \\ &\quad + \frac{Threat\ Intelligence\ Level}{3} \\ &\quad + \frac{Incident\ Response\ Level}{3} \end{aligned}$$

Methodological Justification: The simplified averaging approach for CIN environments reflects a deliberate methodological choice grounded in practical considerations specific to critical infrastructure assessments. Unlike IT, OT, and CT environments, where organizations typically maintain comprehensive technical data enabling precise factor quantification, critical infrastructure environments frequently operate under classified threat environments, governmental security protocols, and operational constraints limiting detailed technical disclosure. The simplified three-factor model prioritizes *qualitative assessment maturity* over false precision in quantification. Organizations applying this formula should conduct separate factor assessments using established methodologies (CMM, NIST, ISO 27001) and then convert qualitative maturity levels to numerical scales (1–5) before aggregation [13–15, 20]. Each component is assessed on a 1–5 scale reflecting cumulative organizational capability:

- **Cybersecurity Maturity Level:** Overall organizational maturity of policies, processes, and security controls (1=initial/ad-hoc; 5=optimized)
- **Threat Intelligence Level:** Capability to gather, analyze, and act upon threat intelligence (1=none; 5=predictive/foresight)
- **Incident Response Level:** Preparedness and effectiveness of incident response (1=reactive; 5=proactive with full automation)

Worked Example:

Assume critical infrastructure organization with: Maturity=4, Threat Intelligence=3, Incident Response=5

$$CRSI_{CIN} = \frac{4+3+5}{3} = \frac{12}{3} = 4.0$$

Interpretation (on 1–5 scale): A CIN achieving CRSI of 4.0 demonstrates strong overall resilience; advancement priorities include threat intelligence capability development and cross-sector information sharing initiatives. Organizations at this level should seek to elevate threat intelligence from a reactive to a predictive posture.

5. Assessment Protocol and Implementation Roadmap

5.1. Assessment Protocol and Subjectivity Mitigation

The framework openly acknowledges what many cybersecurity assessment methodologies implicitly ignore: organizational self-assessment introduces significant subjectivity that can bias results and undermine the framework's utility. Organizations may unconsciously (or consciously) overstate capabilities, misunderstand assessment criteria, or conflate intentions ("we're planning to implement X") with actual implementation. This recognition represents intellectual honesty rather than framework weakness.

5.1.1. *Recommended Assessment Protocols*

Organizations should implement the following assessment protocols to minimize subjectivity and enhance result reliability:

- **Internal Assessment Phase (Baseline):**

  Conduct factor-by-factor assessment using detailed rubrics defining capability expectations at each level. Require multiple assessors from different organizational functions (IT, security, operations, audit). Document the assessment basis with specific evidence.

- **External Audit Phase (Validation and Objectivity):**

  Engage independent third-party auditors to validate internal assessment through technical testing and document review. Conduct penetration testing to validate technical control claims.

- **Continuous Monitoring Phase (Real-Time Refinement):**

  Implement ongoing monitoring of key indicators (vulnerability discovery rates, patch timeliness). Establish quarterly review cycles, refreshing assessment scores based on current evidence.

5.1.2. *External Audit Framework*

Organizations seeking credible, defensible CRSI scores should engage external auditors following this framework:

- **Technical Validation (40% of audit effort):** Penetration testing, configuration review, and log analysis.
- **Procedural Review (35% of audit effort):**

  Policy documentation review, incident response plan testing, and risk assessment methodology validation.

- **Cultural Assessment (25% of audit effort):**

  Staff interviews, training effectiveness measurement, and behavioral observation.

5.2. Technical Implementation Roadmap

Achieving progressive maturity levels requires the systematic execution of specific technical, process, and organizational tasks. The framework identifies 100 specific implementation tasks distributed across ten maturity levels.

5.2.1. *Foundational Infrastructure (Levels 1–2 Tasks)*

- **Level 1 Tasks (Basic Measures):** Network segmentation, firewall configuration (default-deny), MFA deployment, vulnerability scanning, patch management, baseline security configuration, encryption (at-rest/in-transit), and traffic monitoring

- **Level 2 Tasks (Enhanced Detection):** IDS/IPS deployment, penetration testing, EDR implementation, SIEM deployment, formal incident response procedures, secure coding practices, and DLP implementation.

5.2.2. *Advanced Capabilities (Levels 3–4 Tasks)*

- **Level 3 Tasks (Advanced Controls):** Zero-trust architecture, deception technologies, threat intelligence platforms, SOAR, application whitelisting, and SOC establishment.
- **Level 4 Tasks (Strategic Integration):** Cyber risk management frameworks, bug bounty initiatives, DevSecOps practices, threat hunting programs, and advanced security architecture reviews.

5.2.3. *Excellence and Innovation (Levels 5–10 Tasks)*

- **Level 5 Tasks (Strategic Excellence):** AI/ML threat detection, cyber war games, innovation labs, and continuous monitoring platforms.

Figure 2. CRSI Assessment Protocol Flowchart

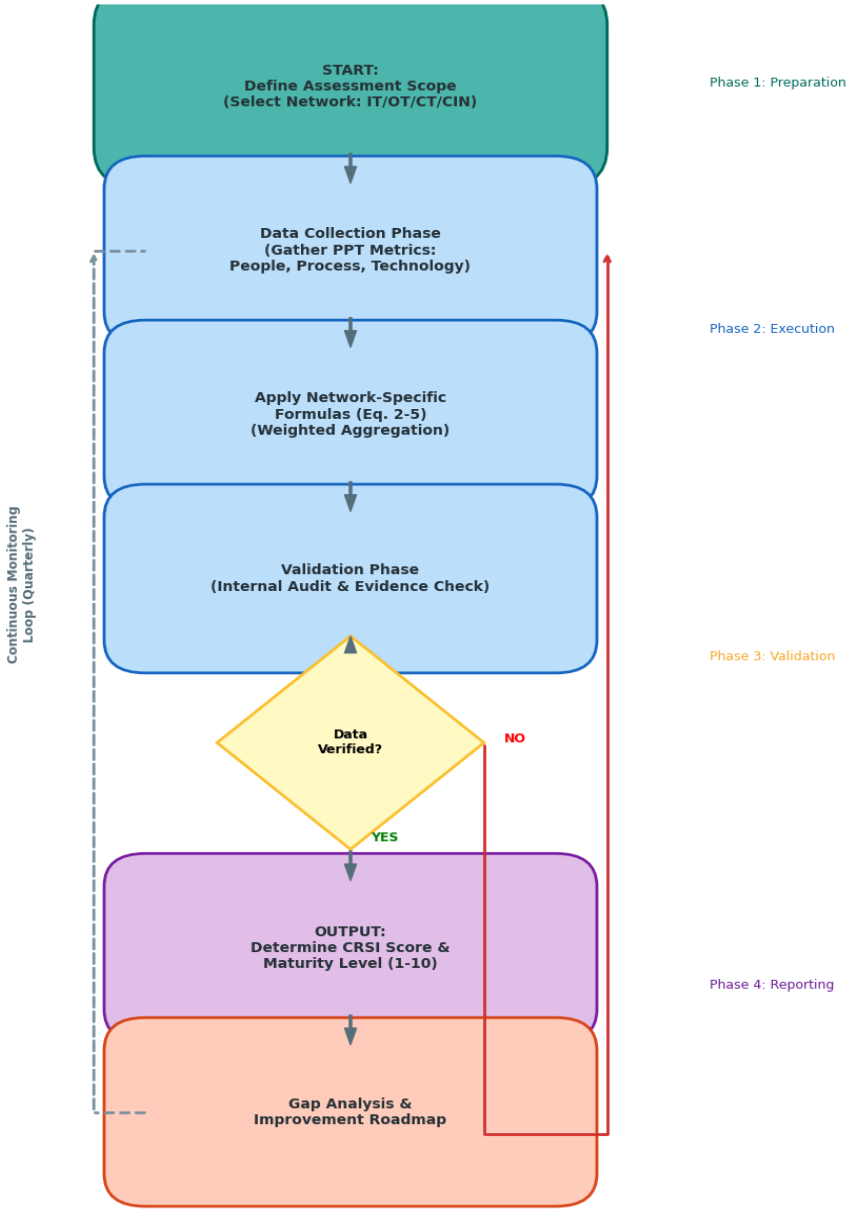

Figure 2. The operational workflow of the CRSI assessment protocol, detailing the transition from data collection to continuous improvement loops

10.57647/ijeee.2026.1701.04

- **Levels 6–10 Tasks (Pinnacle to Zenith):** Quantum-safe cryptography preparation, security centers of excellence, threat intelligence fusion centers, and global resilience coalitions.

6. Simulation Case Study and Validation Protocol

To demonstrate the practical applicability and diagnostic utility of the CRSI framework, we applied the proposed methodology to "EnergyTech," a simulated model of a mid-sized energy utility company operating a hybrid environment (IT enterprise networks and OT control systems). This simulation aims to validate the framework's sensitivity to capability gaps and its ability to quantify resilience improvements over time.

6.1. Baseline Assessment (Scenario A)

EnergyTech initially relied on traditional compliance-based assessments. Upon applying the CRSI-IT formula [Equation 2], the organization scored highly in Firewall Configuration (FW) but poorly in Network Configuration Management (NC) and Privileged Access Management (PAM) due to a lack of automated baseline monitoring.

Input Data: NC=4, IDS=6, FW=9, SIEM=5, PAM=3, NAC=5.

CRSI-IT Calculation:

$$CRSI_{IT} = 0.2(4) + 0.3(6) + 0.1(9) + 0.2(5) + 0.1(3) + 0.1(5) = 5.3$$

Diagnosis: The score of 5.3 places the organization in the "Basic Resilience" (Level 2) category, highlighting a critical vulnerability in internal movement controls (PAM and NC) despite strong perimeter defenses (FW).

6.2. Strategic Improvement Simulation (Scenario B)

Guided by the CRSI findings, the organization shifted its budget allocation. Instead of upgrading the already robust Firewall (which would offer diminishing returns), resources were directed toward implementing automated Configuration Management and deploying a PAM solution.

- Post-Intervention Data:
  - NC: Improved from 4 to 8 (via automation).
  - PAM: Improved from 3 to 7 (via MFA and session recording).
  - Other variables remained constant to isolate the impact.
- Re-Calculation:

$$CRSI_{IT(New)} = 0.2(8) + 0.3(6) + 0.1(9) + 0.2(5) + 0.1(7) + 0.1(5) = 6.5$$

Result: The overall score rose to 6.5, elevating the organization to "Moderate Resilience" (Level 3). This demonstrates the framework's ability to reward "internal hardening" over "perimeter reliance."

PAM and NC) despite strong perimeter defenses (FW).

6.3. Ongoing Empirical Validation and Comparative Protocol

While the EnergyTech simulation demonstrates the functional logic of the CRSI framework, establishing broad ecological validity requires empirical verification across diverse real-world environments. Consequently, a multi-organizational validation study is currently in the data collection phase.

Study Protocol: The ongoing study involves a cohort of eight organizations selected from distinct sectors (Banking, Healthcare, and Industrial Manufacturing). The validation methodology includes:

1. Construct Validity (Comparative Benchmarking): Organizations are subjected to parallel assessments using both the CRSI Framework and the NIST Cybersecurity Framework (CSF 2.0) to measure the correlation between CRSI quantitative scores and NIST Tier assignments.
2. Inter-Rater Reliability (IRR): To address assessment subjectivity, each organization is evaluated independently by two separate audit teams. The consistency of the scoring is measured using Cohen's Kappa coefficient, aiming for an IRR > 0.75.
3. Longitudinal Analysis: Participating organizations will be monitored over a 12-month period to track the sensitivity of the CRSI index to implemented remediation efforts compared to static checklist improvements.

6.4. Sensitivity Analysis and Model Robustness

To evaluate the stability of the CRSI framework against subjective variations in weighting assignments, a sensitivity analysis was conducted. The objective was to determine if minor fluctuations in the weighting coefficients (w_i)—specifically for high-impact factors like IDS ($w = 0.30$)—would result in disproportionate swings in the final resilience score or alter the designated maturity level.

4. Methodology: The weight of the dominant factor (IDS) was varied by $\pm 20\backslash\%$
(ranging from 0.24 to 0.36), while proportionally adjusting the remaining weights to maintain unity ($\sum_{i=1}^{n} w_i = 1.0$). The "Scenario B" data from the EnergyTech case study was used as the baseline.
Sensitivity Metric: The robustness is quantified using the CRSI Sensitivity Range (R_s):

$$R_s = (CRSI_{\Delta w}) - (CRSI_{\Delta w})$$

Results: As illustrated in Figure 4, varying the IDS weight by $\pm 20\backslash\%$

resulted in a minimal score deviation of only ± 0.15 points (Range: 6.38 to 6.62). Crucially, the organization remained within the "Moderate Resilience" (Level 3) band throughout the variation. This indicates that the CRSI framework is robust; it does not generate false "maturity jumps" based on minor subjective weight adjustments, confirming the reliability of the constructed index.

7. Limitations and Future Research Directions

While the CRSI framework offers a significant advancement in quantifying organizational cyber resilience, several inherent limitations warrant discussion to ensure appropriate application and guide future research.

7.1. Subjectivity in Qualitative Inputs

Despite the provision of scoring rubrics, the assignment of factor scores (f_i) relies partially on auditor judgment.

Impact Example: A "Halo Effect" may occur where an auditor, impressed by an organization's documentation (Process), unconsciously inflates the score for technical implementation (Technology), potentially leading to a 15-20% overestimation of actual resilience.

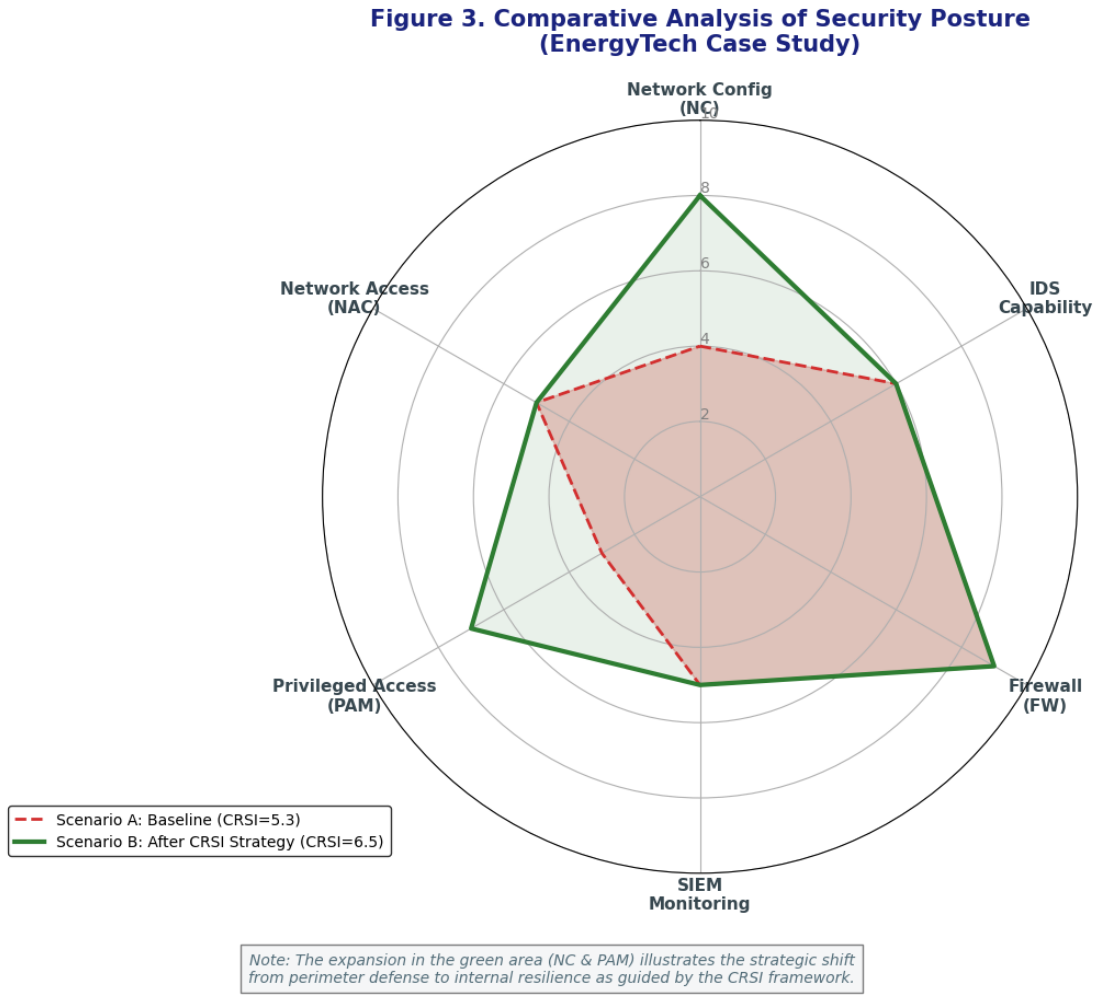

Figure 3. Radar chart visualization of the "EnergyTech" case study, contrasting the baseline posture (Scenario A) with the improved resilience state (Scenario B) achieved through CRSI-guided prioritization

10.57647/ijeee.2026.1701.04

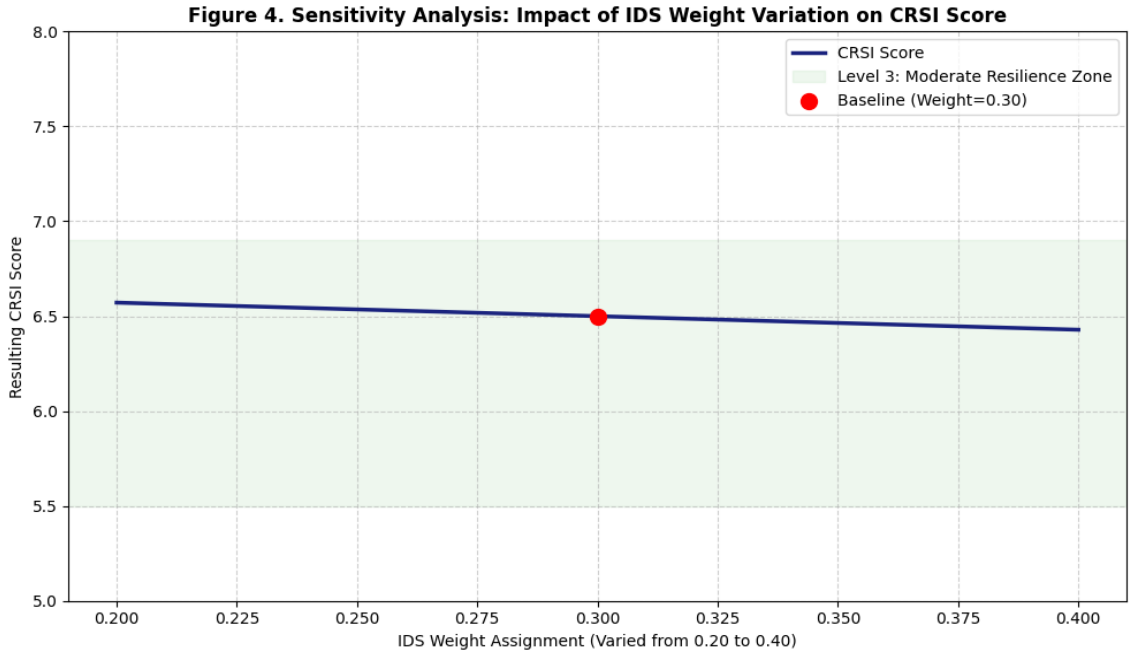

Figure 4. Sensitivity Analysis: Impact of IDS Weight Variation on CRSI Score, demonstrating the model's stability within the 'Moderate Resilience' band despite subjective weighting fluctuations

Current Mitigation: The framework currently advocates for the Inter-Rater Reliability (IRR) protocol (as detailed in Section 6.3) to average out individual biases.

Future Work: Future iterations of CRSI will integrate Natural Language Processing (NLP) to automatically parse security logs and configurations, replacing human inputs with API-driven data collection to ensure objectivity.

7.2. Static Weighting Latency

The current weighting coefficients (w_i) are heuristic, based on annual threat reports (e.g., Verizon DBIR). However, the cyber threat landscape is highly volatile.

Impact Example: If a new zero-day vulnerability emerges that renders Firewalls obsolete overnight, the fixed weight of 0.10 for FW remains static until the next manual recalibration, causing the index to temporarily misrepresent the risk posture.

Current Mitigation: We recommend a quarterly review of weights using the AHP method described in Section 4.2.

Future Work: Developing a Dynamic Weighting Engine using Machine Learning that ingests real-time threat intelligence feeds (e.g., MITRE ATT&CK updates) to adjust weights autonomously in near real-time.

7.3. Operational Overhead for SMEs

The comprehensive nature of the framework, covering IT, OT, and CIN, may present resource challenges for Small and Medium Enterprises (SMEs).

Table 4. Summary of Limitations and Proposed Future Solutions

Domain of Limitation	Operational Impact	Proposed Mitigation Strategy (Future Work)
Assessment Bias	Subjective scoring may inflate resilience levels by ~15%.	Automation: Transition from manual input to API-driven continuous monitoring.
Weight Rigidity	Fixed weights may lag behind rapid shifts in attack vectors.	AI Integration: Reinforcement learning models to dynamically update weights (w_i).
Scope Complexity	High resource demand for data collection in SMEs.	Cloud-Native Tooling: Development of a simplified SaaS platform for automated scoring.

Impact Example: An organization with limited staff may struggle to gather data for all variables in the "CIN" formula, leading to incomplete assessments or "default scoring," which dilutes the diagnostic value.

Current Mitigation: A simplified "Lite" version of the formulas is suggested for organizations below a certain asset threshold.

Future Work: Creation of a SaaS-based CRSI Calculator that streamlines data entry and provides industry benchmarking, reducing the assessment time from weeks to days.

8. Conclusions and Future Research Directions

This research establishes the Cyber Security Resilience Score Index (CRSI) as a quantitative instrument designed to bridge the gap between abstract compliance requirements and operational readiness. By synthesizing the People-Process-Technology dimensions into a unified ten-level maturity model, the framework empowers organizations to transcend static, checklist-based assessments in favor of a dynamic, resilience-centric management approach. The development of distinct mathematical formulations for IT, OT, CT, and critical infrastructure environments ensures that the assessment remains sufficiently granular to support precise diagnostic and strategic planning across diverse network architectures, providing decision-makers with a clear metric to justify security investments.

Advancing beyond the current findings, future research will prioritize the empirical validation of the framework through longitudinal studies that correlate CRSI scores with tangible incident response metrics, such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). Subsequent iterations of the model aim to integrate machine learning algorithms to automate the scoring process using live telemetry data, thereby predicting optimal improvement pathways. Additionally, the scope of the framework is intended to expand to encompass third-party ecosystem resilience, addressing supply chain risks, while simultaneously embedding capabilities for real-time score adjustments driven by dynamic threat intelligence feeds to reflect the volatility of the cyber threat landscape.

Authors Contribution
All authors have contributed equally to prepare the paper.

Availability of data and materials
The data that support the findings of this study are available from the corresponding author, upon reasonable request.

Conflict of interests
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Kott A, Linkov I, editors. Cyber Resilience of Systems and Networks. Cham: Springer International Publishing; 2019. doi: https://doi.org/10.1007/978-3-319-77492-3

[2] Kott A, et al. Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153. 2018.

[3] Galinec D, Steingartner W. Combining cybersecurity and cyber defense to achieve cyber resilience. In: 2017 IEEE 14th International Scientific Conference on Informatics. IEEE; 2017. p. 87–93. doi: https://doi.org/10.1109/INFORMATICS.2017.8327227

[4] Meagher H, Dhirani LL. Cyber-Resilience, Principles, and Practices. 2024. p. 57–74. doi: https://doi.org/10.1007/978-3-031-45162-1_4

[5] Coiciu I, Militaru G. Improvement of Cyber Resilience by Implementation of a Digital Business Continuity Management System: Evidence from Romania. Proc Int Conf Bus Excell. 2024; 18(1): 2492–2505. doi: https://doi.org/10.2478/picbe-2024-0209

[6] AlHidaifi SM, Asghar MR, Ansari IS. Towards a Cyber Resilience Quantification Framework (CRQF) for IT Infrastructure. Comput Netw. 2024; 247: 110446. doi: https://doi.org/10.1016/j.comnet.2024.110446

[7] Khdhir R, et al. Building Resilient National Critical Infrastructure: A Digital Twin-Based Framework for Comprehensive Insider and External Threat Detection. J King Saud Univ Comput Inf Sci. 2026; 38(3): 118. doi: https://doi.org/10.1007/s44443-026-00464-5

[8] Bostick TP, Connelly EB, Lambert JH, Linkov I. Resilience Science, Policy and Investment for Civil Infrastructure. Reliab Eng Syst Saf. 2018; 175: 19–23. doi: https://doi.org/10.1016/j.ress.2018.02.025

[9] Bier V, Gutfraind A. Risk Analysis Beyond Vulnerability and Resilience: Characterizing the Defensibility of Critical Systems. Eur J Oper Res. 2019; 276(2): 626–636. doi: https://doi.org/10.1016/j.ejor.2019.01.011

[10] Aliyu A, et al. A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. Appl Sci. 2020; 10(10): 3660. doi: https://doi.org/10.3390/app10103660

[11] Carías JF, Arrizabalaga S, Labaka L, Hernantes J. Cyber Resilience Progression Model. Appl Sci. 2020; 10(21): 7393. doi: https://doi.org/10.3390/app10217393

[12] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg (MD): NIST; 2018. doi: https://doi.org/10.6028/NIST.CSWP.04162018

[13] Markopoulou D, Papakonstantinou V. The Regulatory Framework for the Protection of Critical Infrastructures Against Cyberthreats: Identifying Shortcomings and Addressing Future Challenges. Comput Law Secur Rev. 2021; 41: 105502. doi: https://doi.org/10.1016/j.clsr.2020.105502

[14] Pesch-Cronin KA, Marion NE. Critical Infrastructure Protection, Risk Management, and Resilience. New York: Routledge; 2024. doi: https://doi.org/10.4324/9781003434887

[15] Gritzalis D, Theocharidou M, Stergiopoulos G, editors. Critical Infrastructure Security and Resilience. Cham: Springer International Publishing; 2019. doi: https://doi.org/10.1007/978-3-030-00024-0

[16] Cao Z, Zhao H, Wang Y, He C, Zhou D, Han X. A Resilience Quantitative Assessment Framework for Cyber–Physical Systems: Mathematical Modeling and Simulation. Appl Sci. 2025; 15(15): 8285. doi: https://doi.org/10.3390/app15158285

[17] Meng D, et al. Security-First Architecture: Deploying Physically Isolated Active Security Processors for Safeguarding the Future of Computing. Cybersecurity. 2018; 1(1): 2. doi: https://doi.org/10.1186/s42400-018-0001-z

[18] Assad A, Moselhi O, Zayed T. A New Metric for Assessing Resilience of Water Distribution Networks. Water. 2019; 11(8): 1701. doi: https://doi.org/10.3390/w11081701

[19] Liu T, Liu F. Graph Neural Networks for Evaluating the Reliability and Resilience of Infrastructure Systems: A Systematic Review of Models, Applications, and Future Directions. IEEE Access. 2025; 13: 164883–164904. doi: https://doi.org/10.1109/ACCESS.2025.3611333

[20] Curt C, Tacnet J. Resilience of Critical Infrastructures: Review and Analysis of Current Approaches. Risk Anal. 2018; 38(11): 2441–2458. doi: https://doi.org/10.1111/risa.13166

[21] Aghazadeh Ardebili A, Lezzi M, Pourmadadkar M. Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. Appl Sci. 2024; 14(24): 11807. doi: https://doi.org/10.3390/app142411807

[22] Wewer G. Bundesamt für Sicherheit in der Informationstechnik (BSI). In: Handbuch Digitalisierung in Staat und Verwaltung. Wiesbaden: Springer Fachmedien Wiesbaden; 2023. p. 1–10. doi: https://doi.org/10.1007/978-3-658-23669-4_104-1

[23] Schiller E, Aidoo A, Fuhrer J, Stahl J, Ziörjen M, Stiller B. Landscape of IoT Security. Comput Sci Rev. 2022; 44: 100467. doi: https://doi.org/10.1016/j.cosrev.2022.100467

[24] Kuzior A, Tiutiunyk I, Zielińska A, Kelemen R. Cybersecurity and Cybercrime: Current Trends and Threats. J Int Stud. 2024; 17(2): 220–239. doi: https://doi.org/10.14254/2071-8330.2024/17-2/12

[25] Verizon. Data Breach Investigations Report (DBIR). New York (NY): Verizon.

[26] European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. Athens: ENISA; 2024.

[27] Casola V, De Benedictis A, Riccio A, Rivera D, Mallouli W, de Oca EM. A Security Monitoring System for Internet of Things. Internet Things. 2019; 7: 100080. doi: https://doi.org/10.1016/j.iot.2019.100080