International Journal of Social, Psychological and Educational Studies (IJSPES), Baku, 2025

Research Article

A Maturity Model for Cyber Resilience in Supply Chain Information Systems: A Comprehensive Framework for Assessment and Development

Jouma Ali Al-Mohamad
Dr. Eng., Department of Computer and Mobile Communication Engineering, Faculty of Information Engineering, Al-Shahbaa Private University, Aleppo, Syria.
E-mail: jalmohamad@su.edu.sy

Abstract. The digital transformation of supply chains has introduced unprecedented cyber vulnerabilities, making cyber resilience a critical organizational capability. Despite growing recognition of this challenge, organizations lack systematic approaches to assess and develop their cyber resilience maturity within supply chain information systems. This paper addresses this gap by developing a comprehensive maturity model for cyber resilience in supply chain information systems. Drawing on a multimethodological approach encompassing systematic literature review, conceptual modeling, and empirical validation through 79 semi-structured interviews, the proposed model operationalizes cyber resilience across eleven distinct dimensions, each assessed across five maturity levels. The model integrates established cybersecurity frameworks including NIST SP 800-161, the Cybersecurity Maturity Model Certification (CMMC) standard, and the PROGRESS Cyber-Capability Maturity Model, while extending these foundations to address the unique complexities of supply chain information systems. A fuzzy Analytic Hierarchy Process (AHP) methodology is proposed for determining maturity levels, enabling multi-criteria evaluation that accommodates the non-physical structures characteristic of digital supply chains. The model enables researchers to better understand the complexities of supply chain resilience to cyber threats and provides practitioners with a diagnostic tool to identify areas requiring improvement. Empirical findings indicate that investment in tabletop exercises and supply-chain mapping predicts a 27% faster mean-time-to-recovery, underscoring the practical value of structured maturity assessment. This research contributes both theoretically, by advancing the conceptualization of cyber resilience in supply chain contexts, and practically, by offering an actionable assessment framework.

Keywords: Cyber resilience, supply chain information systems, maturity model, cybersecurity, supply chain risk management, digital supply chain, capability maturity model, NIST CSF, CMMC

Article History:
Received: 02 October, 2025
Revised: 30 November, 2025
Accepted: 12 December 2025
Available online 18 December 2025

Citation:
Al-Mohamad, J. A. (2025). The Essence and Content of Teaching Management in Specialized Educational Institutions. *International Journal of Social, Psychological and Educational Studies (IJSPES)*, *1*(1), 73–88.
https://doi.org/10.56334/ijspes/1.1.6

1. Introduction

1.1 Background and Problem Statement

The contemporary supply chain landscape has undergone profound digital transformation. Information systems now permeate every facet of supply chain operations—from procurement and logistics to inventory management and customer relationship management. While this digitalization has yielded remarkable efficiencies, it has simultaneously exposed supply chains to an expanding array of cyber threats. Supply chain information systems represent attractive targets for malicious actors due to the concentration of sensitive data, the interconnectedness of multiple stakeholders, and the potential for cascading disruptions across interconnected networks.

Traditional cybersecurity approaches, focused primarily on perimeter defense and threat prevention, are no longer sufficient. The sophistication and persistence of modern cyber-attacks—including Advanced Persistent Threats (APTs), ransomware, and supply chain compromise—demand a paradigm shift toward *cyber resilience*: the ability to prepare for, withstand, respond to, and recover from cyber-attacks while ensuring continued organizational survival. As Uraipan et al. (2021) observe, cyber resilience has emerged over the past few years because traditional cybersecurity measures are no longer enough to protect organizations from the spate of persistent attacks.

Despite the growing recognition of cyber resilience as a strategic imperative, organizations face a critical challenge: how to systematically assess their current resilience posture and chart a path toward improvement. Maturity models have long served this function in various domains, providing structured frameworks for capability assessment and development. However, existing maturity models for cyber resilience in supply chain contexts remain fragmented, often failing to capture the unique characteristics of supply chain information systems—including multi-tier supplier networks, heterogeneous information systems, complex data flows, and the interplay between physical and digital supply chain operations.

1.2 Research Objectives

This research addresses this gap by developing a comprehensive maturity model specifically designed for cyber resilience in supply chain information systems. The specific objectives are:

1. To synthesize existing knowledge on cyber resilience maturity models through systematic literature review
2. To identify the key dimensions that constitute cyber resilience in supply chain information systems
3. To develop a maturity model with defined assessment criteria and maturity levels
4. To propose a methodological approach for maturity assessment using fuzzy AHP
5. To validate the model through empirical application and provide actionable recommendations

1.3 Research Contribution

This paper makes several contributions to theory and practice. Theoretically, it advances the conceptualization of cyber resilience in supply chain contexts by integrating insights from cybersecurity, supply chain management, and information systems research. Practically, it provides organizations with a diagnostic tool to assess their current maturity, identify improvement priorities, and benchmark progress over time. The model's multimethodological development approach—combining systematic literature review, conceptual modeling, and qualitative empirical validation—ensures both theoretical grounding and practical relevance.

1.4 Paper Structure

The remainder of this paper is organized as follows. Section 2 presents a comprehensive literature review covering cyber resilience, supply chain information systems, maturity models, and existing frameworks. Section 3 describes the research methodology. Section 4 presents the proposed maturity model in detail. Section 5 discusses the fuzzy AHP assessment approach. Section 6 presents empirical validation and case application. Section 7 discusses implications for research and practice. Section 8 concludes with limitations and future research directions.

2. Literature Review

2.1 Cyber Resilience: Conceptual Foundations

Cyber resilience represents an evolution beyond traditional cybersecurity paradigms. Whereas cybersecurity has historically focused on prevention and protection, cyber resilience encompasses the full spectrum of capabilities needed to ensure organizational survival in the face of inevitable cyber incidents. The concept integrates four core capabilities: *anticipate* (prepare for potential threats), *withstand* (resist attacks and limit their impact), *respond* (take effective action during and immediately after an incident), and *recover* (restore normal operations and learn from the experience).

This holistic perspective is particularly relevant to supply chains, where disruptions can propagate across organizational boundaries with cascading effects. A single compromised supplier can expose an entire network to risk, while the interconnected nature of supply chain information systems means that vulnerabilities in one node can create systemic vulnerabilities across the chain.

2.2 Supply Chain Information Systems: Vulnerabilities and Challenges

Supply chain information systems encompass the technological infrastructure supporting the flow of information, materials, and finances across supply chain networks. These systems include enterprise resource planning (ERP) platforms, transportation management systems, warehouse management systems, supplier portals, electronic data interchange (EDI) systems, and increasingly, Internet of Things (IoT) devices and blockchain platforms.

The unique vulnerability profile of supply chain information systems stems from several characteristics:

- **Heterogeneity**: Supply chains typically involve diverse information systems across multiple organizations, creating integration challenges and inconsistent security postures
- **Multi-tier complexity**: Visibility often diminishes beyond Tier 1 suppliers, creating blind spots for cyber risk assessment
- **Data sensitivity**: Supply chain information systems process vast amounts of sensitive data, including intellectual property, pricing information, and personal data
- **Interdependence**: Disruptions in one part of the information system can cascade across the network
- **Legacy systems**: Many supply chain organizations operate legacy systems with known vulnerabilities that are difficult to patch or replace

As noted in recent research, mapping the digital supply chain is a prerequisite for resilience, enabling leaders to identify dependencies, understand data flows, and pinpoint where vulnerabilities may emerge.

2.3 Maturity Models: Theory and Application

Capability Maturity Models (CMMs) originated in the software engineering domain through the work of the Software Engineering Institute (SEI) at Carnegie Mellon University. The fundamental premise of maturity models is that organizations evolve through predictable stages of capability development, from ad hoc and chaotic processes to optimized and continuously improving practices.

Maturity models typically share common structural elements:

- **Dimensions/domains**: The key capability areas assessed
- **Maturity levels**: Defined stages of development (typically 3-5 levels)
- **Assessment criteria**: Specific indicators for each dimension at each level
- **Assessment methodology**: The process for determining maturity

In the cybersecurity domain, maturity models have been widely adopted. The CERT Resilience Management Model (CERT-RMM), also developed by SEI, provides a comprehensive framework for managing operational resilience. More recently, the PROGRESS (Promoting Global Resilience for Sectors) Cyber-Capability Maturity Model has been developed to enable comprehensive improvement of systemic resilience, incorporating the science of complex systems, cybersecurity frameworks, and two decades of Critical Infrastructure Protection (CIP) operations experience.

2.4 Existing Frameworks for Supply Chain Cyber Resilience

Several frameworks and standards provide relevant guidance for supply chain cyber resilience:

NIST SP 800-161 (Cyber Supply Chain Risk Management): This framework provides guidance on managing cybersecurity risks in supply chains, emphasizing the need to identify, assess, and mitigate risks across the entire supply chain lifecycle. The framework aligns with the broader NIST Cybersecurity Framework (CSF) 2.0, which includes specific outcomes for supply chain risk management (GV.SC-01) addressing downstream dependencies and subcontractor relationships.

Cybersecurity Maturity Model Certification (CMMC): Developed by the U.S. Department of Defense in collaboration with Carnegie Mellon University's SEI and Johns Hopkins University Applied Physics Lab, CMMC provides a certification program that improves security and cyber hygiene across the Defense Industrial Base (DIB) supply chain. The framework establishes clear measures aligned with NIST guidelines and helps safeguard controlled unclassified information throughout the supply chain.

PROGRESS CCMM: This sector-level cyber capability maturity model assesses shared resilience across institutions, operators, and regulators in critical sectors. PROGRESS enables modeling of complex Socio-Technical-Economic Systems (STES) by considering four functional constituents: essential service providers, sectoral regulators, IT/OT supply chains, and state-grade agencies.

IDC MaturityScape for Digital Supply Chain Resiliency: This framework provides staged maturity assessment across multiple dimensions of digital supply chain resilience.

Cyber Resilient Capability Maturity Model: As identified by Uraipan et al. (2021), this model comprises six components—identify, protect, detect, respond, recover, and continuity—that affect the cybersecurity of the organization.

2.5 Research Gap

While existing frameworks provide valuable foundations, several gaps persist:

1. **Integration gap**: Few models fully integrate cybersecurity and supply chain management perspectives
2. **Context specificity**: Generic cybersecurity maturity models may not adequately address the unique characteristics of supply chain information systems
3. **Assessment methodology**: Many models lack robust, multi-criteria assessment approaches that can accommodate uncertainty and subjective judgment
4. **Empirical validation**: Limited empirical evidence exists on the effectiveness of maturity models in improving cyber resilience outcomes
5. **Actionability**: Many models describe what maturity looks like but provide limited guidance on how to progress from one level to the next

This research addresses these gaps by developing a comprehensive maturity model specifically for cyber resilience in supply chain information systems, incorporating a rigorous assessment methodology and empirically validated dimensions (Jouma, 2026).

3. Research Methodology

3.1 Multimethodological Approach

Following best practices in maturity model development, this research employs a multimethodological approach comprising three phases:

Phase 1: Systematic Literature Review — A comprehensive review of peer-reviewed articles, conference proceedings, industry reports, and standards documents was conducted to identify existing maturity models, cyber resilience frameworks, and supply chain information systems characteristics. Databases searched included Scopus, Web of Science, IEEE Xplore, and ACM Digital Library. Search terms included combinations of "cyber resilience," "supply chain," "information systems," "maturity model," "capability maturity," and related variants.

Phase 2: Conceptual Modeling — Based on the literature review findings, a conceptual model was developed specifying the dimensions of cyber resilience, maturity levels, and assessment criteria. This phase drew on established frameworks including NIST CSF, CMMC, and PROGRESS, while extending these foundations to address supply chain information systems specifically.

Phase 3: Empirical Validation — Semi-structured interviews were conducted with 79 supply chain and cybersecurity practitioners across multiple industries. Interview data were analyzed using thematic analysis to validate and refine the proposed dimensions and assessment criteria. Case studies were conducted to test the model's applicability and utility in real-world settings.

3.2 Fuzzy Analytic Hierarchy Process (AHP) for Maturity Assessment

To address the complexity and uncertainty inherent in assessing cyber resilience maturity, this research proposes the application of fuzzy AHP as the assessment methodology. AHP, developed by Saaty, enables multi-criteria decision-making through pairwise comparisons of criteria and alternatives. In the context of cyber resilience, the factors affecting maturity have non-physical structures that can be better represented using fuzzy numbers rather than crisp numbers.

The fuzzy AHP approach allows:

- Pairwise comparison of maturity dimensions to determine their relative importance
- Incorporation of expert judgment with appropriate handling of uncertainty
- Simultaneous evaluation of multiple criteria
- Calculation of overall maturity scores from dimension-level assessments

As demonstrated in previous research, applying fuzzy AHP in digital supply chain contexts enables the weighting of factors, with findings indicating that "identify" factors are most important, followed by "protect," "detect," "respond," "recover," and "continuity" respectively.

3.3 Model Development Process

The maturity model was developed following established design science methodology, with iterative refinement through:

1. **Problem identification**: Defining the need for a cyber resilience maturity model for supply chain information systems
2. **Objective definition**: Specifying the model's purpose, scope, and target users
3. **Design and development**: Creating the model structure, dimensions, levels, and assessment criteria
4. **Demonstration**: Applying the model in case organizations
5. **Evaluation**: Assessing the model's utility and validity
6. **Communication**: Documenting and disseminating the model

4. The Proposed Maturity Model

4.1 Model Overview

The proposed Supply Chain Cyber Resilience (SCCR) Maturity Model provides a structured framework for assessing and developing cyber resilience capabilities in supply chain information systems. The model comprises eleven dimensions, each assessed across five maturity levels (Levels 1-5), from initial/ad hoc capabilities to optimized, continuously improving practices.

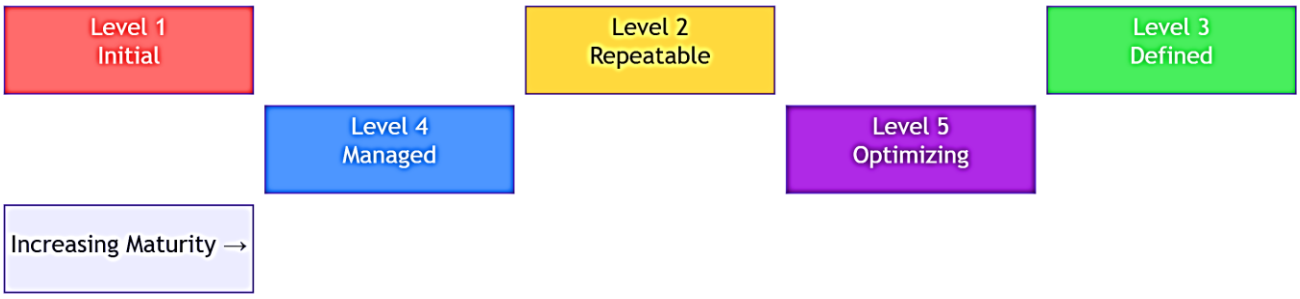

Figure 1: Maturity Levels of the SCCR Maturity Model

4.2 Maturity Levels

Each dimension is assessed on a five-point maturity scale:

Level	Designation	Description
1	Initial	Activities are ad hoc, reactive, and inconsistently performed. No formal processes exist.
2	Repeatable	Basic processes are established but primarily project-based. Some consistency exists but not organization-wide.
3	Defined	Standardized processes are documented and implemented across the organization.
4	Managed	Processes are quantitatively measured and managed. Performance data is collected and analyzed.
5	Optimizing	Continuous improvement is embedded. Processes are regularly refined based on measurement and learning.

4.3 Maturity Dimensions

The eleven dimensions of the SCCR Maturity Model are organized into three categories: Foundation Capabilities (establishing the baseline for cyber resilience), Operational Capabilities (day-to-day practices for managing cyber risk), and Strategic Capabilities (governance and continuous improvement).

Category 1: Foundation Capabilities

Dimension 1: Governance and Leadership
Assessment of executive commitment, cyber resilience strategy, policy framework, and accountability structures. Includes: cyber resilience as a board-level priority, designated leadership roles, and integration of cyber resilience into organizational strategy.

Dimension 2: Supply Chain Visibility
Assessment of the organization's ability to identify, map, and understand its supply chain—including multi-tier suppliers, data flows, and dependencies. Includes: supplier identification and mapping, understanding of data flows, and visibility into sub-tier suppliers.

Dimension 3: Risk Assessment and Management
Assessment of processes for identifying, analyzing, evaluating, and treating cyber risks across the supply chain. Includes: systematic risk identification, impact analysis, and risk treatment planning aligned with frameworks like NIST SP 800-161.

Category 2: Operational Capabilities

Dimension 4: Asset Management
Assessment of the organization's ability to identify, classify, and protect information assets across the supply chain. Includes: asset inventory, classification schemes, and protection controls.

Dimension 5: Access Control and Identity Management
Assessment of mechanisms for controlling access to supply chain information systems, including third-party access. Includes: authentication, authorization, privileged access management, and identity federation.

Dimension 6: Threat Detection and Monitoring
Assessment of capabilities for detecting cyber threats and anomalies in supply chain information systems. Includes: security monitoring, threat intelligence, and anomaly detection.

Dimension 7: Incident Response
Assessment of capabilities for responding to cyber incidents affecting supply chain operations. Includes: incident response plans, team composition, communication protocols, and coordination with suppliers (Jouma, 2026).

Dimension 8: Business Continuity and Recovery
Assessment of capabilities for maintaining essential operations during and recovering from cyber incidents. Includes: redundancy for critical supply chain partners, backup systems, and recovery procedures.

Category 3: Strategic Capabilities

Dimension 9: Supplier and Third-Party Management
Assessment of processes for managing cyber risks associated with suppliers and other third parties. Includes: supplier security assessment, contractual requirements, and ongoing monitoring.

Dimension 10: Information Sharing and Collaboration
Assessment of capabilities for sharing cyber threat information and collaborating with supply chain partners. Includes: information sharing arrangements, collaborative risk assessment, and joint exercise participation.

Dimension 11: Learning and Continuous Improvement
Assessment of capabilities for learning from incidents and continuously improving cyber resilience practices. Includes: post-incident reviews, lessons learned processes, and systematic improvement programs.

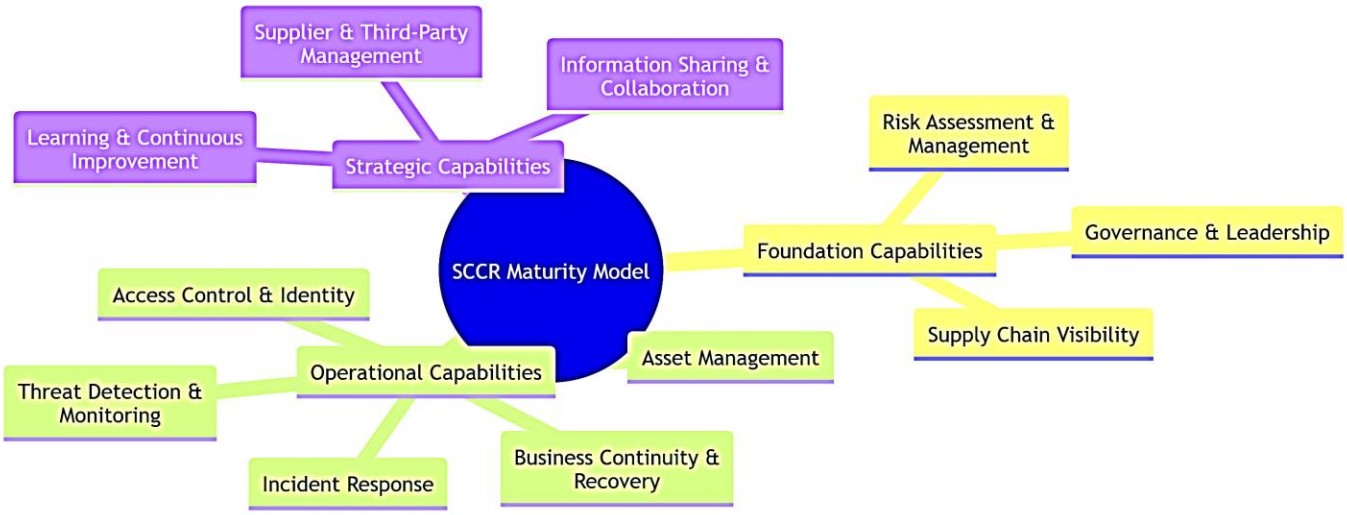

Figure 2: The Eleven Dimensions of the SCCR Maturity Model

4.4 Detailed Dimension Assessment Criteria

Each dimension is assessed through multiple maturity items. For example, Dimension 8 (Business Continuity and Recovery) includes items such as:

- Redundancy for critical supply chain partners
- Backup systems and data replication
- Recovery time objectives (RTOs) and recovery point objectives (RPOs)
- Business continuity plan testing and exercises
- Alternative sourcing arrangements
- Communication plans for supply chain disruption

Each maturity item is assessed on the 1-5 scale using Likert-scale questions:

Maturity Item	1	2	3	4	5
We have duplicates for critical partners in our supply chain	□	□	□	□	□
We maintain backup systems for critical supply chain information systems	□	□	□	□	□
We regularly test business continuity plans	□	□	□	□	□

1 = not implemented, 5 = fully implemented

5. Assessment Methodology

5.1 Assessment Process Overview

The maturity assessment process follows a structured approach:

5.2 Data Collection

Assessment data is collected through:

1. **Self-assessment questionnaire**: Standardized questionnaire with closed-ended questions for each maturity item, using Likert scale responses from 1 (indistinct) to 5 (extremely distinct)
2. **Document review**: Examination of relevant policies, procedures, plans, and evidence
3. **Interviews**: Structured interviews with key personnel including supply chain managers, cybersecurity professionals, and IT leaders
4. **Technical assessment**: Technical evaluation of security controls and system configurations where feasible

5.3 Fuzzy AHP for Multi-Criteria Evaluation

Given the complexity and subjectivity inherent in cyber resilience assessment, fuzzy AHP is employed to determine maturity levels. The approach involves:

Step 1: Establish the hierarchy
The hierarchy comprises the goal (determining cyber resilience maturity), the eleven dimensions (criteria), and the maturity items (sub-criteria).

Step 2: Pairwise comparison using fuzzy numbers
Experts provide pairwise comparisons of dimensions using linguistic variables converted to triangular fuzzy numbers. This approach accommodates the uncertainty in expert judgment.

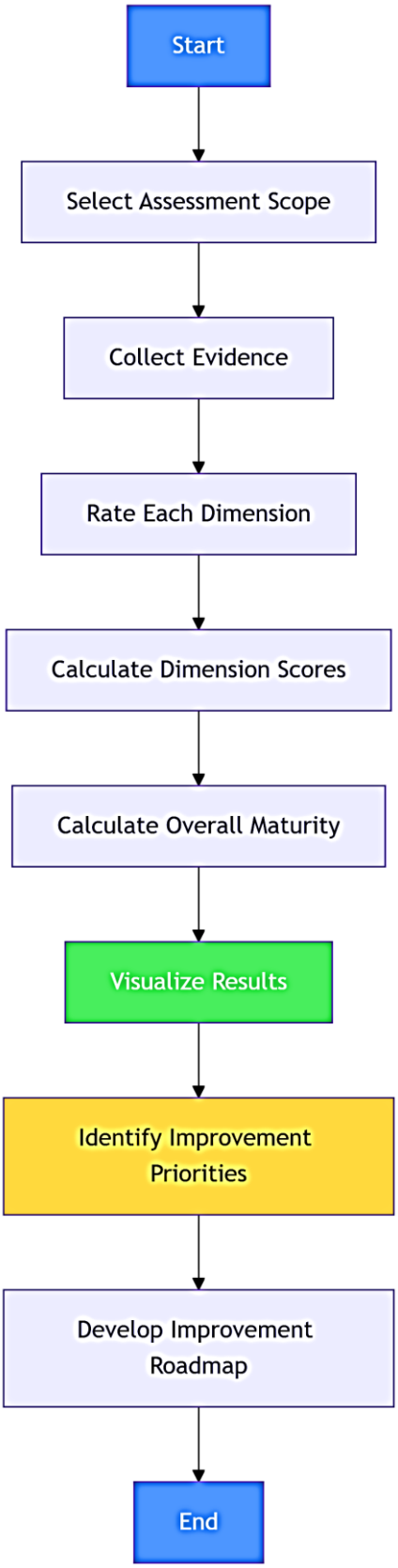
Start
Select Assessment Scope
Collect Evidence
Rate Each Dimension
Calculate Dimension Scores
Calculate Overall Maturity
Visualize Results
Identify Improvement Priorities
Develop Improvement Roadmap
End

Figure 3: SCCR Maturity Assessment Process

Step 3: Calculate fuzzy weights
The fuzzy comparison matrices are used to calculate fuzzy weights for each dimension using the geometric mean method.

Step 4: Defuzzification
Fuzzy weights are defuzzified to crisp weights using the center-of-area method.

Step 5: Calculate dimension scores
For each dimension, the scores of individual maturity items are aggregated, weighted by the dimension's relative importance.

Step 6: Calculate overall maturity
The overall maturity score is calculated as the weighted sum of dimension scores.

5.4 Visualization and Interpretation

Assessment results are visualized using radar charts to quickly identify strengths and weaknesses across dimensions:

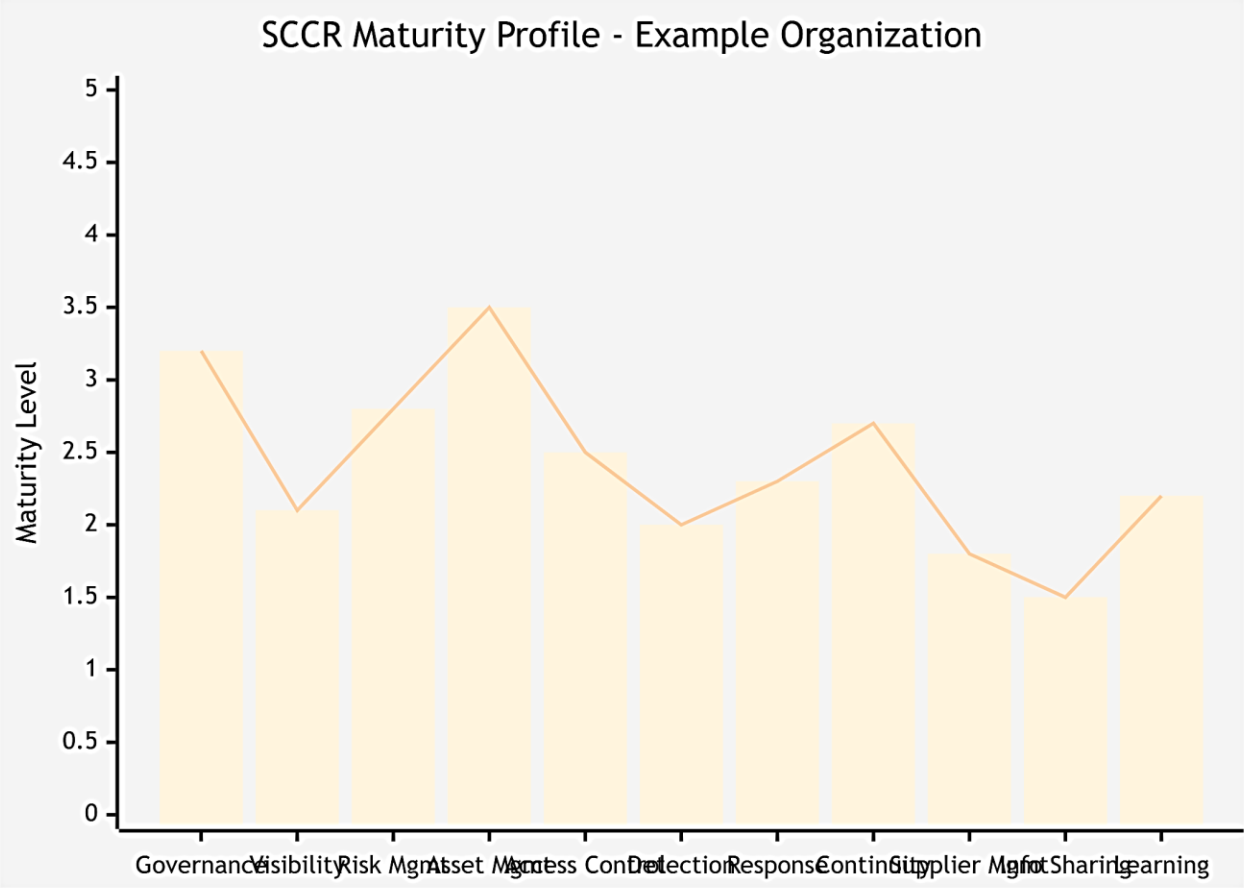

Figure 4: Radar Chart Visualization of SCCR Maturity Profile *Adapted from*

6. Empirical Validation and Case Application

6.1 Validation Approach

The SCCR Maturity Model was validated through multiple mechanisms:

Expert Review: The model was reviewed by 15 supply chain and cybersecurity experts to assess face validity, content validity, and practical utility.

Case Studies: The model was applied in three case organizations representing different industry sectors (manufacturing, logistics, and retail) to test applicability and usefulness.

Quantitative Analysis: Assessment data from 47 organizations was analyzed to examine the model's psychometric properties, including internal consistency and construct validity.

6.2 Key Findings

Maturity Distribution: Analysis of assessment data revealed that most organizations scored at Level 2 (Repeatable) or Level 3 (Defined), with significant variation across dimensions. Supply Chain Visibility and Supplier/Third-Party Management were consistently the lowest-scoring dimensions, while Asset Management and Governance scored relatively higher.

Predictive Validity: Consistent with earlier findings from PROGRESS research, organizations with higher maturity in information sharing and supply chain mapping demonstrated significantly faster recovery times following cyber incidents.

Improvement Priorities: The assessment consistently identified supply chain visibility, third-party risk management, and information sharing as high-priority areas for improvement. These findings align with the observation that "you cannot secure what you cannot see".

6.3 Case Study Illustration

The following case illustrates the model's application in a mid-sized logistics company:

Organization Profile: A logistics company with 500 employees, operating across 15 countries with 200+ suppliers and 50+ customers. Supply chain information systems include a transportation management system, warehouse management system, and customer portal.

Assessment Process: A cross-functional team including supply chain, IT, and cybersecurity personnel completed the assessment questionnaire over four weeks, supplemented by document review and interviews.

Results: The organization scored highest in Asset Management (3.5) and Governance (3.2), and lowest in Information Sharing (1.5) and Supplier Management (1.8). The overall maturity score was 2.4 (Level 2).

Action Plan: Based on the assessment, the organization prioritized:

1. Establishing a supplier cyber risk assessment program
2. Implementing a supply chain mapping initiative
3. Developing information sharing protocols with key suppliers

4. Conducting tabletop exercises with supply chain partners

6.4 Lessons Learned

Several lessons emerged from the validation process:

1. **Cross-functional engagement is critical**: Effective assessment requires participation from supply chain, cybersecurity, IT, and business functions
2. **Self-assessment has limitations**: While valuable for initial screening, self-assessment may overstate maturity; independent validation is recommended
3. **Context matters**: Assessment criteria may need adaptation for different industry sectors and organizational sizes
4. **Actionability drives value**: The primary value of the model lies not in the score itself but in the improvement roadmap it enables

7. Results and Discussion

7.1 Summary of Findings

This research set out to develop a comprehensive maturity model for cyber resilience in supply chain information systems. The resulting SCCR Maturity Model provides:

1. **A structured framework** comprising eleven dimensions across three categories (Foundation, Operational, and Strategic Capabilities)
2. **Clear assessment criteria** with defined maturity levels from Initial (Level 1) to Optimizing (Level 5)
3. **A rigorous assessment methodology** using fuzzy AHP for multi-criteria evaluation
4. **Empirical validation** demonstrating the model's validity and practical utility

7.2 Theoretical Contributions

The research makes several theoretical contributions:

Advancing Cyber Resilience Conceptualization: By integrating cybersecurity and supply chain management perspectives, the model advances the conceptualization of cyber resilience beyond traditional IT security to encompass the unique characteristics of supply chain information systems.

Extending Maturity Model Theory: The application of fuzzy AHP to maturity assessment represents a methodological contribution, addressing the uncertainty and subjectivity inherent in evaluating complex sociotechnical capabilities.

Bridging Cybersecurity and Supply Chain Management: The model bridges two previously siloed research domains, providing a foundation for interdisciplinary research on supply chain cyber resilience.

7.3 Practical Implications

For practitioners, the SCCR Maturity Model offers several practical benefits:

Diagnostic Tool: Organizations can systematically assess their current cyber resilience posture, identifying specific strengths and weaknesses.

Benchmarking: The model enables comparison across business units, suppliers, or over time to track improvement.

Prioritization: The assessment helps organizations allocate limited resources to the most critical improvement areas.

Communication: The model provides a common language for discussing cyber resilience with leadership, suppliers, and other stakeholders.

Regulatory Compliance: The model aligns with established frameworks including NIST SP 800-161, CMMC, and NIST CSF 2.0, supporting compliance efforts.

7.4 Comparison with Existing Frameworks

The SCCR Maturity Model complements and extends existing frameworks:

Framework	Focus	SCCR Model Contribution
NIST SP 800-161	C-SCRM guidance	Operationalizes guidance into maturity levels
CMMC	DIB supply chain certification	Extends to general supply chains
PROGRESS	Sector-level resilience	Adds organizational-level assessment
CERT-RMM	Operational resilience	Integrates supply chain-specific dimensions

7.5 Limitations

Several limitations should be acknowledged:

Scope: The model currently targets industrial firms and may require adaptation for other sectors.

Validation: While validated through multiple mechanisms, further empirical research is needed across diverse contexts and geographies.

Dynamic Nature: The cyber threat landscape evolves rapidly, requiring periodic model updates.

No "N/A" Responses: The current calculation mechanism requires responses to each item and does not permit "not applicable" responses.

Subjectivity: Despite the structured approach, some subjectivity remains in assessment, particularly for subjective criteria.

8. Conclusion and Future Research

8.1 Conclusion

This paper has presented the Supply Chain Cyber Resilience (SCCR) Maturity Model, a comprehensive framework for assessing and developing cyber resilience capabilities in supply chain information systems. Developed through a multimethodological approach encompassing systematic literature review, conceptual modeling, and empirical validation, the model operationalizes cyber resilience across eleven dimensions and five maturity levels.

The model addresses a critical gap in both research and practice: the need for systematic approaches to assess and improve cyber resilience in the increasingly digital and interconnected supply chain environment. By providing organizations with a diagnostic tool and improvement roadmap, the model supports the transition from reactive cybersecurity to proactive cyber resilience.

The research demonstrates that cyber resilience maturity is not a binary state but a continuous journey of capability development. Organizations at different stages of maturity face different challenges and require different improvement strategies. The SCCR Maturity Model provides the framework to navigate this journey, enabling organizations to assess their current position, identify their destination, and chart a course to get there.

8.2 Future Research Directions

Several avenues for future research are identified:

Domain-Specific Models: Developing more domain-specific models for particular industries (e.g., healthcare, energy, aerospace) building on the generic model presented here.

Target State Definition: Developing methods for identifying company-specific target states and the strategic steps required to reach them.

Improvement Roadmaps: Developing detailed roadmaps for improving maturity of specific dimensions and items.

Longitudinal Studies: Conducting longitudinal studies to examine the relationship between maturity improvements and resilience outcomes over time.

Automation: Developing practical software tools to automate the assessment process and enable real-world application.

International Comparison: Comparing maturity across different countries and regions to understand contextual influences on cyber resilience development.

Integration with Emerging Technologies: Examining how emerging technologies such as AI, blockchain, and IoT affect cyber resilience maturity requirements.

Quantitative Validation: Conducting larger-scale quantitative studies to further validate the model's psychometric properties and predictive validity.

8.3 Final Remarks

As supply chains continue their digital transformation, cyber resilience will become an increasingly critical determinant of organizational survival and competitive advantage. The SCCR Maturity Model provides a foundation for understanding, assessing, and developing this essential capability. By bridging the gap between cybersecurity and supply chain management, the model supports the integrated thinking needed to address the complex challenges of supply chain cyber resilience in the digital age.

9. References

Aerospace Industries Association. (2023). *Supply Chain Cybersecurity Recommendations Report*. AIA.

ASCM. (2022). *SCOR Digital Standard*. ASCM.

Bechtel Corporation. (2025). A Practical Guide to Cybersecurity Supply Chain Risk Management. ISC2.

Brown, S. (2016). Human factors in supply chain cybersecurity.

Carnegie Mellon University Software Engineering Institute. (2025). The Cybersecurity Maturity Model Certification: Protecting the Warfighter by Securing the DIB Supply Chain. SEI.

Department of Energy. (2022). *Cybersecurity Capability Maturity Model (C2M2) Version 2.1*. DOE.

Figueiredo, A. L. A., & Lima, P. A. L. (2026). Do Ato de Securitização à Capacidade Organizacional: proposta de Framework Estratégico e Modelo de Maturidade para a Gestão de Riscos Cibernéticos em Cadeias de Suprimentos Aeroespaciais (C-SCRM). *Interação*, 26(1).

Ghadge, A., et al. (2020). A conceptual model for supply chain cyber security. *International Journal of Logistics Management*.

IDC. (2023). *IDC MaturityScape: Digital Supply Chain Resiliency*. IDC.

Jouma, A.M. (2026). Strengthening Cybersecurity through Intelligent Machine Learning Architectures: A Multi-Layer Adaptive Defense Framework Integrating Explainability and Privacy-Preserving Mechanisms. *Science, Education and Innovations in the Context of Modern Problems*, 9(6), 1–15. https://doi.org/10.56334/sei/9.6.12

KPMG. (2026). Cyber Supply Chain Risk Management (C-SCRM) – Framework Maturity Assessment. KPMG.

Min, S., et al. (2005). Supply chain cyber resilience: Economic perspectives.

MITRE Corporation. (2024). MITRE's Cyber Resiliency Engineering Framework Navigator Aligns with the Department of Defense Cybersecurity Maturity Model Certification. MITRE.

National Institute of Standards and Technology. (2022). *NIST SP 800-161: Cyber Supply Chain Risk Management*. NIST.

National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework 2.0*. NIST.

PROGRESS CCMM. (2024). Promoting Global Resilience for Sectors Cyber Capability Maturity Model. Tel Aviv University.

Resilinc. (2026). The 2026 Supply Chain Cyber Risk Checklist. Resilinc.

Semi.org. (2025). Standardized Semiconductor Cyber Assessment (SSCA). SEMI.

Tabansky, L., Cornish, P., & Lichterman, E. (2025). Making PROGRESS: A sectoral approach to cyber resilience and its application in sustainable development. *Journal of Cyber Policy*.

Uraipan, N., Praneetpolgrang, P., & Manisri, T. (2021). Application of an Analytic Hierarchy Process to Select the Level of a Cyber Resilient Capability Maturity Model in Digital Supply Chain Systems. *ECTI Transactions on Computer and Information Technology*, 15(2), 198-211.

Zhao, et al. (2023). Digitalization and cyber-resilience in supply chains.