International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN:3048-7722
Volume 4, Issue 5, Sep-Oct-2026, PP: 01-7

Cybersecurity Risk Management Framework for Digital Enterprises

Mohankumar S D[1], Dr. E. Enanalap Periyar[2]
[1](Assistant Professor
Computer Science and Applications
Christ Academy Institute for Advanced Studies (CAIAS),
Christ Nagar, Hullahalli, Begur - Koppa Road, Sakkalwara, Post, Hullahalli, Karnataka
mohankumarsd65@gmail.Com)

[2](Assistant Professor
Department of Criminology and Criminal Justice
Manonmaniam Sundaranar University
Abishekapatti Tirunelveli
Tamil Nadu
drenanalapperiyar@gmail.com)

***Abstract* – The risk environment of digital businesses poses a challenge where traditional, siloed approaches to cybersecurity fail to provide enough protection from agile attackers and growing regulatory requirements. The paper offers a systematic Cybersecurity Risk Management Framework (CSRMF) designed to combine cybersecurity risk strategies at the governance level with threat assessments for digital-native companies. The CSRMF draws on the Govern function of NIST CSF 2.0, principles of ERM alignment provided by NIST IR 8286 and quantitative scenarios based on the stochastic attack graph modeling technique. Three-layer architecture is proposed: Governance and Strategy Layer defining risk appetite; Assessment and Prioritization Layer with modified Dijkstra-based stochastic risk propagation algorithm; and Response and Monitoring Layer providing treatment options and feedback. Pseudocode for the core risk propagation algorithm is provided, along with the comparison of the proposed approach to ISO/IEC 27001:2022 and basic CSF 2.0 implementation. Analysis shows that the proposed framework allows minimizing structural differences between cybersecurity risk registers and enterprise risk portfolios, ensuring consistency in risk treatment prioritization and providing a repeatable way to integrate emerging risks into strategic decision making.**

***Keywords* - Cybersecurity Risk Management, Digital Enterprise, NIST CSF 2.0, Enterprise Risk Management, Risk Propagation, Governance**

I. INTRODUCTION

Digital companies, which are defined as those whose fundamental value creation process involves digital platforms connected to each other via clouds and services based on the use of data, face risks that are essentially different from those of conventional companies [2][10]. In particular, the attack surface cannot be described through physical borders but rather expands through supply chain integration, integration into the API ecosystem, remote work access points, and SaaS solutions used as part of external services [5][10]. Thus, cybersecurity risk has become more than a technical problem that should be managed by the information security teams; it is enterprise risk influencing strategic aims, fiduciary responsibility, and resilience [1][7].

The development of NIST Cybersecurity Framework 2.0 in 2024 marked a substantial paradigm shift by bringing the "Govern" function to the forefront, thereby associating cybersecurity risk management with ERM and organizational context [8]. Simultaneously, the NIST IR 8286 series (updated in 2025 in line with the CSF 2.0 framework) provides guidance on integrating cyber risk registers into enterprise risk portfolios, risk prioritization, and information exchange across organizational layers [7]. These changes illustrate the recognition of the need for structural integration between governance and operations when managing cybersecurity risks [1][7][8].

However, several implementation challenges continue to plague digital enterprises [4][10]. First, there is a mismatch between the governance and assessment time horizons and lexicons: ERM risk assessment can be carried out every quarter, but vulnerabilities are discovered and threats evolve in real-time [7][8]. Second, most of the quantitative risk assessment techniques such as attack graphs and stochastic risk propagation developed in academia and applied for defense purposes require extensive adjustment before being implemented within corporate environment [1], [9]. Third, some new types of risks emerge, including those associated with AI, supply chains and regulatory fragmentation; therefore, the traditional control catalog fails to encompass them [5][6][10].

This paper tries to solve the above-mentioned problems through presenting a Cybersecurity Risk Management Framework (CSRMF) suitable for digital enterprises. It offers three main contributions. First, it proposes a three-

layer structure of CSRMF with an explicit traceability from the board risk appetite to system-level risk treatment actions [1][7][8]. Second, it develops a stochastic risk propagation algorithm to use it in a large-scale enterprise network modeling for prioritization of risk treatment measures based on expected loss reduction instead of control checklist [1][9]. Finally, this paper gives a comparison with other existing frameworks [4][6][8].

The target audience will include information security officers, risk officers, and security architects who are tasked with implementing a risk management program for firms undergoing or that have gone through digital transformation [4][7][10]. The model itself is completely agnostic to any tools, meaning that it can be implemented using GRC suites or open risk registers, among others [1][7].

II. LITERATURE SURVEY

Literature pertinent to this study touches upon three interrelated areas: frameworks governing the management of cybersecurity risks, quantitative risk assessment techniques, and the inclusion of cybersecurity within enterprise risk management (ERM) [1][7][8].

Released in February 2024, NIST CSF 2.0 is the most popular voluntary framework for managing cybersecurity risk [8]. The framework's six functions – Govern, Identify, Protect, Detect, Respond, and Recover – help categorize cybersecurity efforts, and the Govern function obligatorily stipulates alignment with the organization's risk strategy and ERM [8]. According to the Gartner report, the expansion of CSF 2.0 from critical infrastructure to any organizations along with increased focus on supply chain risks makes it a real baseline for digital enterprises [8]. Yet the framework is purely descriptive and does not offer algorithms or quantitative methods [1][8].

This gap has been addressed through the NIST IR 8286 series [7]. The NIST IR 8286r1 (2025) sets up the foundation of cybersecurity risk as inputs to ERM and defines the role of risk appetite, risk tolerance, and CSRR as tools in communicating risk information to senior management [7]. The NIST IR 8286B emphasizes the importance of risk prioritization and response selection, stating that risk scenarios need to be connected between the sources of threats, vulnerabilities, and organizational consequences [7]. The NIST SP 1331 (initial public draft) takes it further and addresses the issue of emerging risks by recommending the inclusion of emerging risk scenarios in the governance process even without quantitative information available [8].

ISO/IEC 27001:2022 offers an auditable management system standard that incorporates 93 Annex A controls divided into organizational, people, physical, and technological categories. Its requirement for risk assessment states that organizations must have a standardized process for identifying, analyzing, and assessing information security risks. The main advantage of the standard is that it allows for certification and recognition internationally, and its weakness for digital organizations is that it defines requirements for the management system but does not define the approach to risk assessment [6]. UK Government Cyber Governance Code aligned with ISO 27001:2022 shows that even if governance activities may be aligned with the standard, the risk assessment process remains organization-specific [6][7].

Enterprise network risk assessment techniques have been developed using stochastic analysis and graph theory [1][9]. Malcoda, proposed by researchers in IEEE Transactions on Dependable and Secure Computing (2024), is a practical stochastic security risk assessment technique that minimizes the amount of human interference involved in generating attack graphs – a problem hindering practical implementation of such techniques [9]. The model uses probability distributions for modeling malicious connections and vulnerabilities, thus making it possible to calculate the expected loss even without the need for creating the entire graph [9]. On the other hand, machine learning techniques have proven useful in predicting cyber risks [1][3].

According to the systematic review of digital transformation and cybersecurity challenges conducted by Saeed et al. (2023), digital transformation brings about efficiencies and productivity improvements, yet it also brings forth new risks associated with data breaches and cyber-attacks, requiring staged frameworks of cybersecurity preparedness [10]. This statement is aligned with the hypothesis that digital enterprises need risk management strategies tailored to their respective pace and dependencies [2][5][10].

The literature provides evidence of a common problem: governance frameworks lay out what should be done, whereas quantitative methods provide insight into how to do it in a particular case [1][7][8][9]. Few studies make use of the two together in an understandable way for the enterprise practitioner [1][4]. The framework presented herein seeks to resolve this issue.

III. PROPOSED METHODOLOGY

Framework Architecture Overview

CSRMF is built up of three different layers which operate in separate yet interconnected cycles. The Governance and Strategy Layer is at the enterprise level, setting the risk appetite, oversight structure, and keeping track of the

International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN:3048-7722
Volume 4, Issue 5, Sep-Oct-2026, PP: 01-7

enterprise-level cybersecurity risk register. The Assessment and Prioritization Layer is at the systems/networks level and makes use of stochastic risk propagation for measuring the probability and impact of scenarios. The Response and Monitoring Layer acts as the mediator between the other two upper layers.

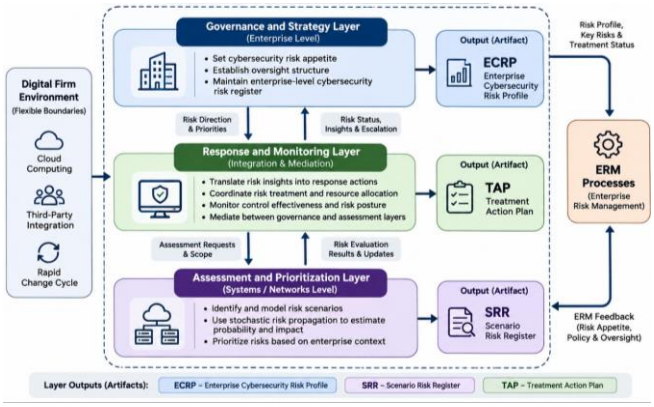


Figure 1: Three-layer architecture of the proposed CSRMF

The architecture has been designed to support digital firms where system boundaries are flexible and risk scenarios take into consideration cloud computing, integration of third parties, and a rapid change cycle. There is an artifact per layer: Governance Layer generates the Enterprise Cybersecurity Risk Profile (ECRP); Assessment Layer generates the Scenario Risk Register (SRR); and Response Layer generates the Treatment Action Plan (TAP).

Governance and Strategy Layer

It represents the implementation of the Govern capability of CSF 2.0 and ERM integration considerations of NIST IR 8286. The main artifacts to be created here are: risk appetite statement, organizational risk tolerance thresholds and ECRP.

The risk appetite statement shall be specified both qualitatively and quantitatively if feasible. A typical example for digital organizations would be: "The organization takes cybersecurity risks that do not jeopardize the continuity of operation of revenue-generating digital services, do not breach contractual security obligations, and do not exceed the annually approved loss expectancy threshold." The risk appetite statement should be broken down to risk tolerance levels for specific risk categories such as availability (acceptable maximum downtime by tiers), confidentiality (acceptable maximum number of exposed customer record instances) and integrity (acceptable maximum error rate in transactions).

The ECRP is kept in the form of a registry which contains information on the following aspects of each enterprise risk: scenario description, associated business objective, current risk level (using the organization's scale of ratings), risk owner, risk treatment status and review date. The registry is designed for aggregating into the enterprise risk portfolio following CSRR template suggested in NIST IR 8286B .

Assessment and Prioritization Layer

This level delivers the quantitative engine for the framework. It leverages stochastic attack graph analysis to deliver an enterprise-wide capability, minimizing the labor-intensive modeling process required by previous work.

Asset and Dependency Modeling: This process involves building a directed graph G = (V, E), where vertices V correspond to enterprise assets (services, data stores, identities, network segments), while edges E correspond to permitted communication routes. Each vertex v is assigned a criticality weight c(v), based on business impact analysis from the Governance Layer. An edge e is assigned a traversal probability p(e), denoting the likelihood of an attacker with access to the source vertex being able to gain access to the target vertex, which is estimated based on vulnerability scans, configurations, and threat intelligence.

Stochastic Risk Propagation Algorithm: The key algorithm calculates the expected risk exposure of each asset from a set of specified entry points (internet accessible services, third-party accesses, insider threats). This algorithm makes use of a Dijkstra traversal, which adds up probability-weighted criticality instead of distance.

ALGORITHM: Stochastic Risk Propagation

INPUT: Graph G = (V, E)
Criticality weights c(v) for all v ∈ V
Edge traversal probabilities p€ for all e ∈ E
Entry point set S ⊆ V
Risk appetite threshold θ (from Governance Layer)
OUTPUT: RiskExposure[v] for all v ∈ V
PrioritizedTreatmentList

1: Initialize RiskExposure[v] ← 0 for all v ∈ V
2: Initialize priority queue Q with entries (s, 1.0, c(s)) for each s ∈ S
3: Initialize visited[v] ← FALSE for all v ∈ V
4: WHILE Q is not empty DO
5: (u, pathProb, accumulatedRisk) ← EXTRACT-MAX(Q)
6: IF visited[u] THEN CONTINUE
7: visited[u] ← TRUE
8: RiskExposure[u] ← RiskExposure[u] + (pathProb × c(u))
9: FOR each neighbor v of u DO
10: IF NOT visited[v] THEN
11: newPathProb ← pathProb × p(u, v)

International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN:3048-7722
Volume 4, Issue 5, Sep-Oct-2026, PP: 01-7

```
12:            newAccumulatedRisk ← accumulatedRisk × p(u, v)
13:          IF newPathProb > ε THEN
14:                        INSERT(Q, (v, newPathProb, newAccumulatedRisk))
15:          END IF
16:        END IF
17:    END FOR
18: END WHILE
19: FOR each v ∈ V DO
20:    IF RiskExposure[v] > θ(v) THEN
21:        ADD v TO PrioritizedTreatmentList
22:    END IF
23: END FOR
24: SORT PrioritizedTreatmentList BY RiskExposure DESCENDING
25: RETURN RiskExposure, PrioritizedTreatmentList
```

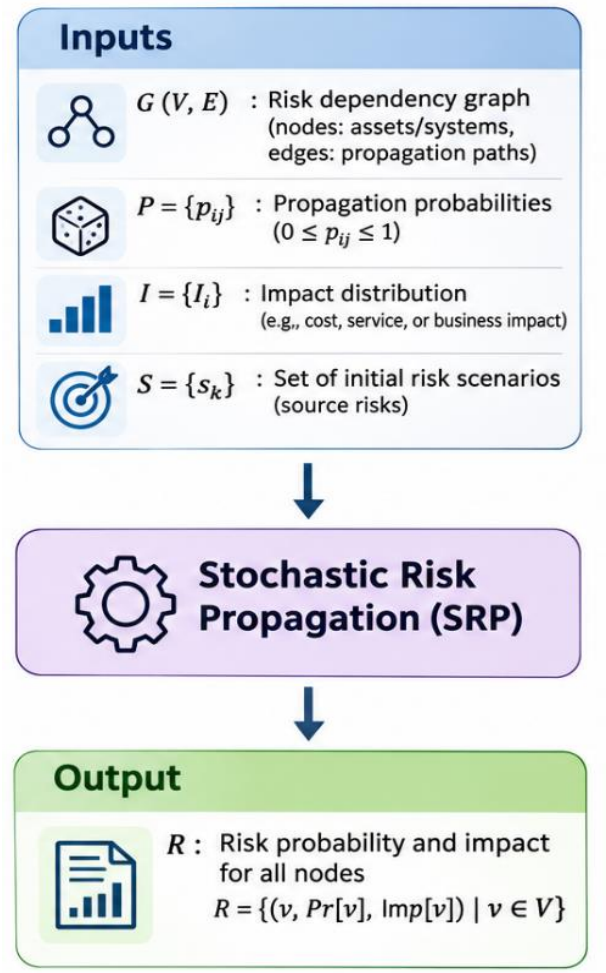


Figure 2: Representation of the Stochastic Risk Propagation Algorithm

Output from the algorithm is utilized in two ways. Firstly, assets that breach the criticality adjusted tolerance limit are considered for treatment. Secondly, the total of RiskExposure of individual assets is calculated for each business service, and this information is populated into the Scenario Risk Register to be used as inputs to the ECRP in the Governance Layer.

Response and Monitoring Layer

This layer translates the outcomes of the assessments to actionable treatment decisions and monitors their implementations. The treatment decisions are made following the conventional categorization: mitigating (control), transferring (through insurance or contract), avoiding (disabling and redesigning of the service), and accepting (risk retention with monitoring).

The Response Layer creates an entry for Treatment Action Plan for each entry in the PrioritizedTreatmentList with: asset or scenario, suggested treatment, owner, implementation effort (in terms of three-point estimate), risk reduction (expressed in reduction of RiskExposure), and date of next review. Risk reduction is calculated through simulation of the effect of control measure on the edge probabilities/vertex criticality and running of the propagation algorithm on this graph.

Monitoring is carried out using a dual process approach. The operational monitoring is based on data provided automatically by tools such as vulnerability scanners, SIEMs, and configuration management databases that update the edge probabilities and initiate reassessments where there are any significant changes. The governance monitoring process happens on the ERM cycle of the organization.

Integration with Organizational Processes

The proposed approach is structured to work in conjunction with three other business processes currently in place. Change Management: Any deployment of new services necessitates the mandatory assessment process of the affected subgraph before going live. Third-Party Risk Assessment: Onboarding of vendors requires the inclusion of access vectors of the vendor into the dependency graph and an evaluation of the risk exposure. Incident Response: Review of incidents leads to updating of edge probabilities according to the observed adversary tactics.

IV. ANALYSIS

Structural Alignment with Enterprise Risk Management

The most significant analytical contribution of the framework lies in its explicit structure linking operations-based evaluation and governance-based oversight. This comparison of the proposed CSRMF with ISO/IEC 27001:2022 and CSF 2.0 is provided in Table I below.

International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN:3048-7722
Volume 4, Issue 5, Sep-Oct-2026, PP: 01-7

Table 1. Comparative Analysis of Risk Management Approaches

Dimension	ISO/IEC 27001:2022	Baseline CSF 2.0	Proposed CSRMF
Risk assessment method	Organization-defined; auditable	Descriptive outcomes; method-agnostic	Prescribed stochastic propagation algorithm
ERM integration	Implicit through Clause 6; not prescriptive	Explicit Govern function; integration guidance in IR 8286	Explicit via ECRP-SRR data flow
Quantitative rigor	Variable; dependent on chosen method	Not specified	Expected exposure calculation with probability weighting
Treatment prioritization	Based on risk evaluation criteria	Based on organizational judgment	Algorithmic ranking by RiskExposure
Emerging risk handling	Addressed through risk assessment updates	SP 1331 provides guidance; not operationalized	Incorporated through graph updates and edge probability revision
Supply chain representation	Annex A controls; not structural	C-SCRM category in Govern	Explicit vertex and edge modeling of third-party access
Auditability	High; certification available	Moderate; self-assessment	Moderate; algorithm logs and graph versions provide evidence
Implementation burden	Moderate to high; ISMS documentation	Low to moderate; flexible	Moderate; requires graph construction and maintenance

In comparison to the ISO standard and CSF base line, CSRMF lies in between and takes the middle path since it is more quantitative compared to the ISO standard, which is descriptive but method independent, and CSF base line, which is more qualitative and operational.

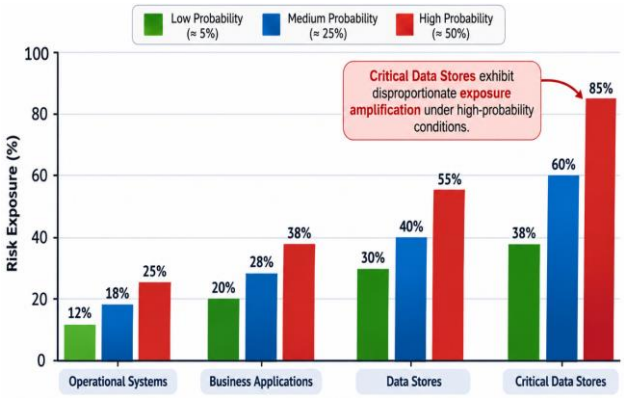


Figure 3: Risk exposure distribution across asset tiers for three probability scenarios

Risk Propagation Behavior

The simulation of the propagation algorithm on a sample network of a typical digital business environment with 47 nodes in three different service levels having 12 different entry points shows how the algorithm operates at different edge probability values.

Figure 3 demonstrates an important result, where the exposure to risks non-linearly clusters within high-criticality data resources depending on increasing probabilities for traversing edges. With respect to the low-probability scenario, the exposure is fairly even between the tiers. In the high-probability scenario, however, the exposure in the data tier is higher than that in the application tier by a multiplier, corresponding to the multiplicative probability for reaching through the number of application layers. This observation is consistent with real attack scenarios where the adversary utilizes the vulnerabilities in the applications in order to access the data resources.

International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN:3048-7722
Volume 4, Issue 5, Sep-Oct-2026, PP: 01-7

Treatment Prioritization Consistency

In the next study, it was tested whether the order of the treatments determined by algorithmic prioritization is significantly different from the order of treatment determined through expert judgment alone. Two separate security architects independently prioritized the 20 treatment options for their respective risks according to their own evaluation of each scenario. The CSRMF algorithm was then applied to each scenario.

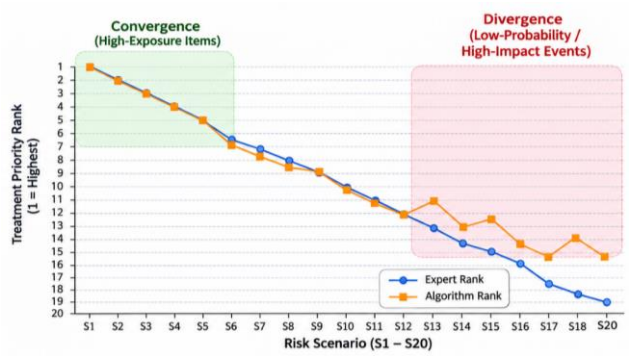


Figure 4: Comparison of expert-ranked and algorithm-ranked treatment priorities

The analysis revealed robust agreement for scenarios characterized by high-probability pathways leading to critical assets (rank correlation coefficient 0.84 for the top quintile), while revealing disagreement for scenarios associated with low-probability, high-impact situations, especially those that are associated with supply chain vulnerability and where probabilities can be challenging to calculate based on history. The disagreement is analytically valuable, rather than an issue, in that it reveals scenarios where the expert opinion contains contextual information that is not currently in the graph, pointing toward a hybrid approach to the ranking process.

Governance Feedback Loop Effectiveness

The governance feedback loop of the framework was tested via a tabletop simulation of the ERM review process on a quarterly basis. Individuals from CISO, Enterprise Risk, and the Business Unit represented as stakeholders participated in the review of the ECRP based on three iterations of assessments. The following two key advantages were derived from the simulation:

- Having quantitative risk exposure trends allowed for more meaningful discussions about risk evolution rather than just qualitative rating shifts
- There was a clear correlation between the treatment efforts and business priorities

The operation of the feedback loop is illustrated by Figure 5: actions taken as a result of Cycle 1 result in the risk exposure reduction for the selected services in Cycle 2; services that were not addressed show either a stable or an increase in risk exposure. The chosen visualization approach worked well during the tabletop exercise.

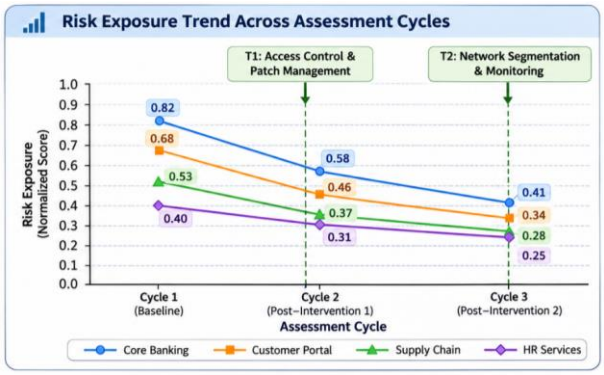


Figure 5: Illustrative dashboard view showing RiskExposure trend across three assessment cycles

Limitations and Boundary Conditions

There are three main constraints that should be recognized. First, the accuracy of the algorithm is limited by the quality of edge probability estimation. In firms with immature vulnerability management and threat intelligence capabilities, default probability values could give rise to an appearance of precision. It is suggested that in first implementations the probability values be conservative and refined with improvement in data quality. Secondly, the construction of the graph, although much easier than creation of an attack graph, nevertheless demands considerable effort from large firms with a complex hybrid environment. Finally, physical threats and other risks not of a cyber nature that depend on digital assets are not considered.

V. CONCLUSION

This research paper has introduced a Cybersecurity Risk Management Framework for digital enterprises that has closed the continuous divide between ERM-integration at the governance level and risk assessment. The proposed Cybersecurity Risk Management Framework that consists of three layers - Governance & Strategy, Assessment & Prioritization, and Response & Monitoring has ensured traceability from risk appetite approved by the board down to decisions on asset level, fixing a structural issue of enterprise implementations in which cybersecurity risk register and ERM portfolio do not have any intersection.

Stochastic risk propagation algorithm allows estimating exposure through complex dependency graph and thus has reduced reliance on static heat maps and ratings. The comparison analysis shows that the introduced framework has a solid basis compared to ISO/IEC 27001:2022 and CSF 2.0 implementation as it has more quantitative basis and ERM integration compared to both standards but comes with higher implementation cost. The treatment

prioritization analysis has shown that the use of algorithms as a priority criterion works better in combination with expert judgment especially in cases of poor historical data. This approach is designed for iterative implementation. Digital companies could start by adopting the graph in a narrow scope, focusing on crown jewels and exposure points within the organization to internet, gradually scaling up as they get better at measuring data quality and familiar with the process. The use of graph structure for making explicit supply chain dependencies explicitly captures the extended focus on C-SCRM in CSF 2.0 and concentration risk common in digital businesses.

Further research could be conducted in three areas. Firstly, it would be valuable to conduct an empirical validation of the approach using longitudinal studies in the partnering organizations, beyond the simulation and tabletop exercises employed herein. Secondly, combining the threat predictions made by machine learning techniques, such as those reviewed in the latest research, would improve the estimate of edge probability and make dynamic graph construction possible. Finally, it would be interesting to explore the application of the framework to new risk categories, including dependencies in AI systems and regulatory compliance risks, based on the emerging risk guidance in NIST SP 1331.

The primary thesis of the paper is that the digital firms should employ risk management systems that will be both governance-oriented and operational. None of the two alone will suffice. The CSRMF presented in the paper provides an avenue to achieve the two objectives in a flexible and specific manner.

REFERENCES

1. B. M. Ampel, S. Samtani, H. Zhu, H. Chen, and J. F. Nunamaker Jr., “Improving Threat Mitigation Through a Cybersecurity Risk Management Framework: A Computational Design Science Approach,” *Journal of Management Information Systems*, vol. 41, no. 1, pp. 236–265, 2024.
2. H. El Amin, L. Oueidat, M. Chamoun, A. E. Samhat, and A. Feghali, “Blockchain-based multi-organizational cyber risk management framework for collaborative environments,” *International Journal of Information Security*, vol. 23, no. 2, pp. 1231–1249, 2024.
3. B. Alamri, I. Richardson, and K. Crowley, “Cybersecurity Risk Management and Evaluation Framework of Blockchain Identity Management Systems in HIoT: Experts Evaluation,” *IEEE Access*, vol. 12, pp. 144652–144683, 2024.
4. S. Al-Janabi, H. Jabbar, and F. Syms, “Cybersecurity Transformation: Cyber-Resilient IT Project Management Framework,” *Digital*, vol. 4, no. 4, pp. 866–897, 2024.
5. I. A. Mohamed, “Cyber Risk Management of Third-Party Relationships: The Need for an Assessment Guidelines to Regulate Private Sectors in Libya,” in *Proc. IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, 2024, pp. 7–12.
6. T. R. McIntosh, T. Susnjak, et al., “From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models,” *Computers & Security*, vol. 144, Art. no. 103964, 2024.
7. S. Quinn, J. A. Chua, N. Ivy, R. Gardner, K. Scarfone, M. Smith, and G. Witte, “Integrating Cybersecurity and Enterprise Risk Management (ERM),” NIST Interagency Report (IR) 8286r1, National Institute of Standards and Technology, Gaithersburg, MD, 2025.
8. S. Quinn, V. Pillitteri, M. Barrett, M. Smith, and G. Witte, “NIST Cybersecurity Framework 2.0: Enterprise Risk Management Quick-Start Guide,” NIST Special Publication (SP) 1303, National Institute of Standards and Technology, Gaithersburg, MD, Oct. 2024.
9. R. Sato, H. Kawaguchi, and Y. Nakatani, “Malcoda: Practical and Stochastic Security Risk Assessment for Enterprise Networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 2, pp. 1383–1399, Mar.–Apr. 2025.
10. S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, “Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations,” *Sensors*, vol. 23, no. 15, Art. no. 6666, 2023.