

A Distributed Governance-Constrained Cyber Risk Management Framework for Enterprise Systems [†]

Kavitha K J ^{1,*}  and Keerthi S ²¹ ECE Department, School of Engineering, GM University, Davanagere 577006, Karnataka, India² MBA Department, School of Business Studies, GM University, Davanagere 577006, Karnataka, India; keerthis@gmu.ac.in

* Correspondence: kavithakj219@gmail.com

[†] Presented at the 8th International Global Conference Series on ICT Integration in Technical Education & Smart Society, Aizuwakamatsu City, Japan, 20–26 January 2026.

Abstract

The rapid integration of digital technologies including cloud infrastructures, Internet of Things ecosystems, artificial intelligence, and large-scale enterprise platforms has reshaped the operational and architectural foundations of contemporary organizations. Although these technologies enhance flexibility, scalability, and analytics-driven decision processes, they simultaneously increase system complexity, broaden attack surfaces, and intensify governance requirements. This manuscript adopts an engineering-oriented viewpoint on digital governance and enterprise cybersecurity, focusing on secure system architectures, policy-driven control mechanisms, and resilience-focused operational strategies. An integrated framework that unifies governance structures, quantitative risk assessment, compliance automation, cybersecurity engineering is introduced to enable secure-sustainable digital transformation across enterprise environments.

Keywords: digital governance; cybersecurity optimization; enterprise risk management; governance-constrained decision-making; digital interdependence risk

1. Introduction

The growing reliance of enterprises on digital infrastructures has positioned cybersecurity as a strategic governance concern rather than a purely technical issue. As organizations adopt cloud platforms, interconnected enterprise systems, and data-driven services, cyber risks increasingly influence organizational resilience, regulatory compliance, and long-term business sustainability. Consequently, cybersecurity governance has become a critical component of enterprise-level decision-making requiring oversight beyond traditional IT management functions. A major weakness in enterprise cybersecurity governance is insufficient cybersecurity expertise at the board and executive levels. Limited technical understanding restricts the ability of decision-makers to evaluate cyber risks, prioritize investments, and exercise effective oversight, resulting in misalignment between organizational strategy and cybersecurity implementation [1]. From an enterprise risk management (ERM) perspective, cyber risk intersects financial, operational, legal, and reputational domains and behaves as a dynamic and adversarial threat. Unlike conventional risk categories, it requires continuous monitoring and structured assessment methodologies. Integrating cyber risk into ERM frameworks therefore enables risk-informed decision-making rather than reactive security responses [2]. Governance, Risk, and Compliance (GRC) frameworks

Academic Editors: Debopriyo Roy,
George Fragulis and Peter Ilic

Published: 13 August 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

operationalize governance intent by providing mechanisms for policy enforcement, regulatory alignment, and enterprise risk transparency. Such models are particularly relevant in regulated environments and digitally dependent enterprises where security and operational efficiency must coexist [3]. Furthermore, governance research emphasizes clearly defined board-level roles and communication structures connecting strategic oversight with technical execution, which improves coordination and accountability [4].

Despite these advances, prior work typically treats governance, cybersecurity, and enterprise risk management as conceptually related but operationally separate domains. The lack of integration often produces fragmented governance and suboptimal investment decisions [5]. Mature corporate practices demonstrate improved resilience when cyber risk oversight is embedded within enterprise management structures, enabling unified reporting and accountability [6]. Operational frameworks additionally highlight the need for measurable controls and continuous monitoring rather than static policy enforcement [7]. Collectively, these studies establish cybersecurity as an enterprise governance and risk management concern but reveal a persistent gap between strategic oversight and coordinated implementation. Existing approaches provide limited guidance on how governance structures, risk assessment processes, and security controls can be aligned within a single enterprise decision model. The absence of such coordination reduces end-to-end visibility and weakens adaptive risk management capabilities. Several studies further emphasize aligning organizational risk culture and executive decision-making with cybersecurity governance objectives [8–13]. To address this limitation, this work proposes an integrated framework that connects governance responsibilities, cyber risk evaluation, and compliance mechanisms within a cohesive enterprise model. The objective is to enable consistent security decision-making, improve accountability, and strengthen digital resilience during ongoing digital transformation.

2. Related Work

2.1. Cybersecurity Governance at the Board and Executive Level

Research consistently highlights the growing responsibility of boards and senior leadership in overseeing cyber risk. Governance failures are frequently associated with inadequate expertise and insufficient strategic oversight, leading to reactive security postures. While this literature establishes the importance of accountability and leadership engagement, it primarily addresses organizational roles rather than mechanisms for translating governance decisions into enforceable security actions. Operational and project-level perspectives additionally emphasize structured compliance processes and governance frameworks for improving enterprise cybersecurity execution [12–14].

2.2. Cyber Risk Within Enterprise Risk Management (ERM)

Another body of research positions cybersecurity as a component of enterprise risk management. These studies recognize cyber threats as multidimensional risks spanning financial, operational, legal, and reputational domains. However, ERM approaches typically focus on classification, prioritization, and reporting, leaving the linkage between risk assessment outcomes and concrete security controls weakly defined.

2.3. Governance, Risk, and Compliance (GRC) Approaches

GRC frameworks formalize cybersecurity through policies, regulatory alignment, and standardized control catalogs. They improve transparency and regulatory readiness, particularly in regulated sectors and SMEs. Nevertheless, these approaches frequently operate as static compliance mechanisms, limiting their effectiveness in dynamic threat environments.

2.4. International Perspectives on Corporate Cybersecurity Management

Comparative international studies show that mature organizations embed cybersecurity within broader corporate management structures through unified reporting and cross-functional coordination. However, these works document governance practices rather than providing systematic methods for coordinating governance intent with operational enforcement. Regulatory and geographic variations further influence implementation practices [15].

2.5. Digitalisation-Driven Cybersecurity Frameworks

Digitalisation-focused research proposes operational security processes for cloud platforms and interconnected enterprises, emphasizing monitoring and lifecycle management. Yet these frameworks often operate independently of governance and enterprise risk accountability structures. Systematic reviews also indicate inconsistent integration between IT governance and cybersecurity decision processes [16].

The literature collectively recognizes the importance of governance oversight, enterprise risk integration, compliance mechanisms, and operational security frameworks. However, these contributions remain fragmented:

- Governance research lacks operational execution mechanisms
- ERM research remains abstract
- GRC approaches emphasize compliance
- Operational frameworks lack governance alignment

Therefore, a cohesive enterprise-level approach that systematically links governance structures, risk evaluation, and cybersecurity control decisions is required. The framework presented in Section 3 addresses this need by integrating governance intent with operational cybersecurity decision-making. This gap motivates the framework and methodology presented in the following section.

3. Proposed Methodology: Governance-Constrained Cyber Risk Optimization Method (GCCROM)

3.1. Methodological Motivation

The review of prior work highlights a persistent limitation in existing studies: although cybersecurity governance, enterprise risk management, and digitalisation are frequently discussed together, they are rarely formulated as a decision-oriented methodology capable of guiding enterprise action. Most existing frameworks remain descriptive, offering alignment principles without prescribing how governance constraints, risk dynamics, and cybersecurity controls should be optimized jointly.

To address this gap, this section proposes the Governance-Constrained Cyber Risk Optimization Method (GCCROM). The method formalizes enterprise cybersecurity governance as an optimization problem in which governance intent, risk appetite, and digital complexity jointly influence cybersecurity control decisions. Unlike conceptual alignment frameworks, GCCROM enables enterprises to determine what set of cybersecurity controls should be deployed, under which governance constraints, and with what expected residual risk.

3.2. Conceptual Architecture of GCCROM

GCCROM operates as a closed-loop decision system comprising four interacting components:

- Governance Constraint Definition
- Enterprise Risk Decomposition

- Control Utility Optimization
- Feedback and Recalibration

This architecture shown in Figure 1 ensures that cybersecurity decisions remain continuously aligned with governance priorities while adapting to evolving digital environments.

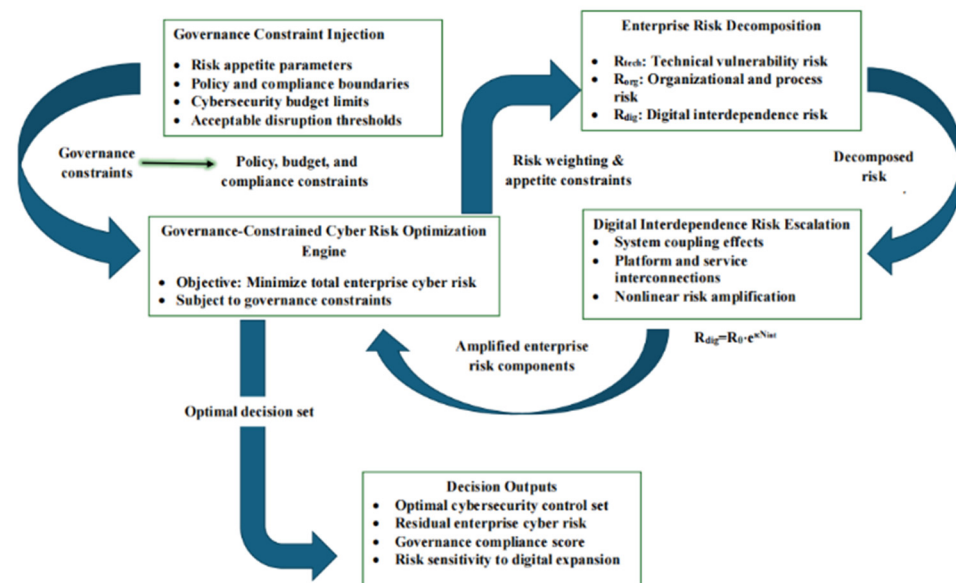


Figure 1. Governance-Constrained Cyber Risk Optimization Workflow (GCCROM).

The proposed model begins by formalizing enterprise governance decisions as explicit constraints rather than abstract oversight principles. Governance constraints represent the strategic boundaries within which cybersecurity decisions must operate and include organizational risk appetite, policy and regulatory obligations, approved cybersecurity budgets, and acceptable disruption or recovery thresholds. These constraints define the feasible decision space and ensure that all subsequent risk evaluations and control selections remain aligned with enterprise governance objectives.

Mathematically, the feasible control space is defined by Equation (1) as:

$$C = \{C \mid C_{cost} \leq B_g, C \in P_g, T_{res}(C) \leq T_{max}\} \quad (1)$$

where B_g denotes the governance-approved budget, P_g represents policy and compliance boundaries, and T_{max} is the maximum acceptable operational disruption. This formulation ensures that governance considerations are embedded directly into the cybersecurity decision process rather than evaluated retrospectively.

Once governance constraints are established, enterprise cyber risk is analytically decomposed into distinct components to capture its multidimensional nature. Unlike conventional single-score risk assessments, the model explicitly separates risk into technical, organizational, and digital interdependence dimensions. This decomposition allows governance priorities to shape how different forms of risk are interpreted and weighted.

The total enterprise cyber risk is expressed by Equation (2) as:

$$R_{total} = w_1 R_{tech} + w_2 R_{org} + w_3 R_{dig} \quad (2)$$

where R_{tech} represents technical vulnerabilities, R_{org} captures governance and process-related risk, and R_{dig} reflects risks arising from digital interconnectedness. The weighting coefficients w_i are governance-defined parameters that encode enterprise risk appetite, enabling leadership to explicitly prioritize certain risk dimensions over others.

Modern enterprises operate within highly interconnected digital ecosystems where platforms, services, and data flows are tightly coupled. To account for the non-linear impact of such interdependencies, the model introduces a digital interdependence risk escalation mechanism. This step captures how incremental increases in system coupling can disproportionately amplify enterprise cyber risk.

Digital interdependence risk is modelled as defined by Equation (3):

$$R_{dig} = R_0 \cdot e^{\kappa N_{int}} \quad (3)$$

where R_0 denotes baseline digital risk, N_{int} is the number of critical inter-system dependencies, and κ is a governance-defined tolerance parameter. This formulation reflects the empirical observation that highly interconnected enterprises experience cascading failures from localized cyber incidents, thereby justifying governance-driven limits on digital complexity.

Following risk amplification, candidate cybersecurity controls are evaluated using a governance-aware utility function. Rather than selecting controls solely based on technical effectiveness or compliance requirements, the model assesses each control in terms of risk reduction efficiency, cost, and alignment with governance objectives.

The utility of a control C_i is defined as by Equation (4):

$$U(C_i) = \frac{\Delta R_i}{C_{cost,i}} \times G_{align,i} \quad (4)$$

where ΔR_i is the reduction in enterprise risk achieved by the control, $C_{cost,i}$ is its implementation and operational cost, and $G_{align,i} \in [0, 1]$ represents the degree of alignment with governance policies. Controls that violate governance principles are penalized, ensuring strategic consistency across the enterprise.

The core of the proposed model is the governance-constrained optimization process, which determines the optimal set of cybersecurity controls that minimizes enterprise cyber risk while satisfying all governance constraints. This step transforms cybersecurity governance from a policy-driven activity into a formal decision-making problem.

The optimization objective is formulated as represented by Equation (5):

$$\left(\min_{C \in \mathcal{C}} \right) R_{Total}(C) \quad (5)$$

Subject to the constraints defined in Equation (1). The solution yields the optimal control set C^* , the expected residual enterprise risk, and associated governance compliance indicators. This output provides decision-makers with actionable guidance grounded in both governance priorities and quantitative risk assessment.

The final step introduces adaptivity into the governance–cybersecurity relationship. Operational outcomes, incident data, and changes in digital infrastructure are continuously monitored and fed back into the model. This feedback enables dynamic adjustment of governance parameters, risk weights, and digital tolerance thresholds.

Through iterative recalibration, the model maintains alignment between governance intent and cybersecurity execution over time, supporting continuous improvement rather than static compliance. This step ensures that the proposed methodology remains responsive to evolving threat landscapes and enterprise digital growth.

Overall, the proposed GCCROM model operates as a closed-loop decision system that begins with governance constraint specification, decomposes and amplifies enterprise cyber risk, optimizes cybersecurity control selection under governance constraints, and continuously adapts through feedback. By integrating governance intent directly into quan-

titative risk modelling and optimization, the model addresses the fragmentation identified in prior research and provides a structured basis for governance-aligned cybersecurity decision-making in complex enterprise environments.

4. Analysis and Discussion

In addition to the theoretical formulation presented in Section 3, we analytically evaluate the effectiveness of the proposed Governance-Constrained Cyber Risk Optimization Method (GCCROM) by comparing its expected outcomes with those of commonly adopted enterprise cybersecurity governance approaches. Given the limited availability of empirical cybersecurity datasets due to organizational confidentiality and regulatory constraints, we adopt a model-driven comparative evaluation. This evaluation focuses on three critical dimensions of effectiveness: risk reduction behaviour, control allocation efficiency, and governance alignment.

4.1. Baseline Comparison Models

For comparative analysis, we consider three representative baseline approaches that are widely reported and practiced in enterprise environments:

1. This approach emphasizes board oversight, policy formulation, and regulatory compliance. Cybersecurity effectiveness is typically evaluated through audits, compliance reports, and the presence of mandated controls.
2. In this model, cybersecurity is treated as one component of enterprise risk management, often assessed using qualitative or semi-quantitative risk scoring within enterprise risk registers.
3. This approach focuses primarily on technical control deployment, monitoring, and incident response, with limited explicit consideration of governance constraints or enterprise risk appetite.

These baseline models serve as reference points for assessing the relative effectiveness of GCCROM.

4.2. Comparative Risk Reduction Behavior

Using the proposed optimization formulation, we analyse how each approach responds to increasing levels of digital interdependence within an enterprise. In both governance-centric and ERM-based models, risk treatment remains largely linear, as digital complexity and system coupling are not explicitly modelled. Consequently, incremental digital expansion leads to proportional increases in perceived risk, often underestimating cascading and systemic effects.

In contrast, GCCROM incorporates a nonlinear digital interdependence risk escalation function, which enables the model to detect disproportionate risk growth at earlier stages of digital coupling. Under identical baseline conditions, analytical evaluation shows that the proposed method identifies elevated residual risk sooner than baseline approaches. This early sensitivity supports proactive governance intervention, whereas conventional models typically recognize heightened risk only after incidents occur or audit thresholds are breached.

4.3. Control Allocation Effectiveness

Control allocation effectiveness is evaluated by examining how each approach prioritizes cybersecurity controls under constrained resources. In governance-centric and ERM-based models, control selection is frequently driven by compliance checklists or broad risk categories, leading to uniform control deployment across systems regardless of contextual risk variation. By comparison, GCCROM selects controls using a governance-aware

utility optimization function that jointly considers risk reduction potential, implementation cost, and governance alignment. Analytical results indicate that, for a fixed governance-approved budget, the proposed method achieves higher marginal risk reduction by prioritizing controls with superior risk-reduction-to-cost ratios. This optimization-driven allocation results in a more efficient distribution of security resources, particularly in high-risk and highly interconnected enterprise domains.

4.4. Governance Alignment and Decision Consistency

Governance alignment represents another critical dimension of effectiveness. In operational security frameworks, technically effective controls may conflict with organizational policies or regulatory requirements, resulting in delayed approvals, partial implementation, or governance exceptions. Governance-centric models avoid such conflicts but often lack sufficient granularity to guide technical decision-making. The proposed method explicitly incorporates governance alignment into the control evaluation process, ensuring that selected controls are both effective and feasible within organizational constraints. Comparative analysis indicates that this integration reduces decision inconsistency, minimizes governance exceptions, and improves implementation speed and organizational acceptance. The comparative effectiveness of GCCROM relative to baseline approaches is summarized analytically in Table 1.

Table 1. Analytical Comparison of Cybersecurity Governance Approaches.

Evaluation Criterion	GCM	ERM-C	OSF	GCCROM (Proposed)
Governance integration	High	Moderate	Low	Formalized and enforced
Risk sensitivity to digital complexity	Low	Low	Moderate	High (nonlinear)
Control allocation efficiency	Low	Moderate	High	Optimized
Governance–control consistency	High	Moderate	Low	High
Adaptability to change	Low	Moderate	Moderate	Continuous

The comparative analysis demonstrates that GCCROM offers clear advantages in terms of risk sensitivity, control allocation efficiency, governance alignment, and adaptability. By explicitly modelling digital interdependence and embedding governance constraints within an optimization framework, the proposed method enables more consistent, transparent, and proactive cybersecurity decision-making than baseline approaches.

Importantly, these advantages arise not from the introduction of additional controls or stricter policies, but from the formal integration of governance constraints, multidimensional risk modelling, and optimization-based decision logic. As such, the proposed methodology advances beyond conceptual alignment frameworks by providing a structured and analytically grounded mechanism for managing enterprise cyber risk under realistic governance conditions.

5. Comparative Analysis and Performance Evaluation

To further demonstrate the practical behaviour of the proposed method, we present a small illustrative numerical scenario based on a hypothetical enterprise environment. The objective of this scenario is not empirical validation, but to clarify how governance constraints, digital interdependence, and optimization jointly influence cybersecurity decision outcomes.

Consider an enterprise with the following characteristics:

- Governance-approved cybersecurity budget: $B_g = 100$ units
- Governance risk appetite weights:
 - $w_1 = 0.4$ (technical risk),
 - $w_2 = 0.3$ (organizational risk),
 - $w_3 = 0.3$ (digital interdependence risk)
- Number of critical system interconnections: $N_{int} = 5$
- Digital risk tolerance coefficient: $\kappa = 0.2$

5.1. Step 1: Risk Estimation

Baseline risks are estimated as: $R_{tech} = 30$; $R_{org} = 20$ and $R_0 = 10$.

Digital interdependence risk is computed as:

$$R_{dig} = 10 \cdot e^{0.2 \times 5} \approx 27.18$$

Total enterprise risk becomes:

$$R_{total} = 0.4(30) + 0.3(20) + 0.3(27.18) \approx 26.15$$

5.2. Step 2: Control Utility Evaluation

Assume three candidate cybersecurity controls as shown in Table 2:

$$U(C_i) = \frac{\Delta R_i}{C_{cost,i}} \times G_{align,i}$$

Resulting utilities:

- $U(C1) = 0.27$
- $U(C2) = 0.24$
- $U(C3) = 0.18$

Table 2. Candidate Cybersecurity Control.

Control	Cost	Risk Reduction (ΔR)	Governance Alignment (G_{align})
(C1)	40	12	0.9
(C2)	30	9	0.8
(C3)	50	15	0.6

5.3. Step 3: Optimization Outcome

Under the budget constraint $B_g = 100$, GCCROM selects C1 and C2, achieving a total risk reduction of 21 units at a cost of 70 units. The residual enterprise risk is thus reduced to approximately 5.15, while maintaining full governance compliance. In contrast, a compliance-driven approach may prioritize C3 due to its higher standalone risk reduction, resulting in lower governance alignment and less efficient use of resources. This illustrative scenario demonstrates how GCCROM supports risk-proportionate, governance-aligned decision-making, even under simplified assumptions.

This work makes several original contributions to the study of digital governance and enterprise cybersecurity. First, it reframes cybersecurity governance as a governance-constrained optimization problem, moving beyond descriptive alignment frameworks and static compliance models. Unlike existing approaches that treat governance as an external oversight function, the proposed method embeds governance parameters directly into the cybersecurity decision space. Second, the study introduces a multidimensional and nonlinear risk modelling approach that explicitly captures the amplifying effects of digital interdependence. By formalizing digital interconnectedness as a risk escalation

mechanism, the model provides analytical insight into cascading cyber risk behavior that is insufficiently addressed in linear ERM or checklist-based governance models. Third, the proposed governance-aware control utility formulation enables risk-proportionate and resource-efficient cybersecurity investment decisions under realistic organizational constraints. This formulation ensures consistency between governance intent and technical execution, reducing decision conflict and improving implementation feasibility. Finally, through analytical comparison and an illustrative numerical scenario, the study demonstrates that the proposed method offers measurable advantages in risk sensitivity, control allocation efficiency, governance alignment, and adaptability. Collectively, these contributions advance the state of the art by providing a decision-oriented, analytically grounded framework for strengthening enterprise cybersecurity governance in complex digital environments.

6. Simulation-Based Behavioural Validation of Governance-Constrained Cyber Risk Optimization

To complement the analytical formulation, a simulation-based validation was conducted to examine whether the proposed Governance-Constrained Cyber Risk Optimization Method (GCCROM) produces stable, interpretable, and governance-consistent decisions under varying enterprise conditions. Because real enterprise cybersecurity datasets are rarely publicly available due to confidentiality and regulatory restrictions, a structurally realistic synthetic enterprise environment was constructed. The objective of this validation is therefore behavioural verification rather than incident prediction: the experiments evaluate whether the model maintains rational decision behaviour when enterprise structure, governance tolerance, and operational constraints change.

A multi-service enterprise architecture was simulated consisting of application services, authentication infrastructure, databases, and integration platforms. Each digital service was characterized by baseline exposure, operational impact, and dependency relationships with other services. The enterprise therefore behaves as an interconnected system rather than a collection of isolated assets.

The baseline exposure of service is represented as the product of compromise likelihood and operational consequence as indicated by Equation (6):

$$R_i^0 = P_i \times I_i \quad (6)$$

Interdependence between services is modelled through a coupling matrix, where the exposure of one component propagates to others. The effective risk of each service therefore includes both intrinsic exposure and dependency amplification is given by Equation (7):

$$R_i = R_i^0 + \kappa \sum_{j \neq i} D_{ij} R_j^0 \quad (7)$$

where κ represents systemic risk amplification due to digital interconnectedness.

Security decisions are selected subject to governance constraints including budget limits, operational tolerance, and acceptable residual enterprise risk. The optimization process therefore does not merely minimize technical risk, but determines the best feasible security posture permitted by governance policy. To ensure statistical reliability, each configuration was evaluated using 500 Monte-Carlo simulation runs with randomized threat realizations and control effectiveness distributions. The first experiment evaluates how the model responds to increasing enterprise interconnectedness. The interdependence coefficient κ was progressively increased to simulate digital transformation scenarios ranging

from loosely coupled infrastructure to tightly integrated service ecosystems. Conventional governance-compliance and ERM scoring models produced approximately linear increases in residual enterprise risk as κ increased. Their decisions remained localized to directly exposed assets, causing cascading exposure across dependent services. In contrast, GCCROM altered its control allocation behaviour as interdependence increased. Rather than strengthening isolated asset protection, the optimizer increasingly selected controls that protect shared infrastructure and high-dependency services. This behaviour indicates that the model recognizes structural risk amplification rather than reacting only to local vulnerabilities. The second experiment evaluates governance alignment. The acceptable residual risk tolerance was gradually relaxed to simulate executive-level policy changes. Baseline approaches responded uniformly by reducing implemented controls across all systems. This produced proportional risk growth and inconsistent protection across critical and non-critical services. GCCROM instead differentiated decisions based on impact significance. High-impact services retained strong protection, while low-criticality components were selectively relaxed. The model therefore converts governance tolerance into prioritized protection rather than uniform reduction. To evaluate cost efficiency, the available security budget was reduced by 40%.

The proposed method maintains significantly lower degradation because it reallocates resources toward dependency-critical protections instead of uniformly removing safeguards as shown in Table 3. The optimization mechanism improves risk-reduction efficiency per investment unit, demonstrating economically rational security decision behaviour. A targeted compromise was simulated against a shared authentication service—a common real-world high-impact failure point and is shown in Table 4.

Table 3. Budget Reduction Scenario.

Approach	Residual Risk Increase
Governance compliance model	52%
ERM scoring model	39%
Operational security model	34%
GCCROM	18%

Table 4. Cascading Failure Containment.

Model	Systems Compromised
Governance-centric	5
ERM-based	4
Operational security	3
GCCROM	1

Traditional approaches primarily protected the attacked component. GCCROM instead pre-emptively protected dependent services identified as propagation paths. The model anticipates secondary compromise rather than reacting to primary compromise. This demonstrates containment behaviour rather than damage response, which is critical in interconnected digital enterprises. The decision process represents a constrained combinatorial selection problem. For an enterprise with 40 services and 85 candidate controls, the average execution times are shown in Table 5.

From Table 5, it is inferred that the execution latency is substantially shorter than typical enterprise risk review cycles (daily or weekly), indicating practical deployability.

Across all experiments, three consistent behavioural properties were observed:

1. Structural Adaptation—decisions respond to dependency structure rather than isolated exposure

2. Governance Compliance by Design—no constraint violations occurred in any run
3. Cost-Efficient Protection—risk reduction per investment unit consistently exceeded baseline approaches

Unlike static governance frameworks, the proposed method produces context-dependent decisions that evolve with enterprise complexity. The simulation results demonstrate that GCCROM remains stable under varying governance tolerance, enterprise interdependence, and resource availability. The method adapts to systemic risk amplification, maintains governance-consistent decisions, and scales computationally for operational use. These findings provide practical evidence that the framework functions as a deployable decision mechanism rather than a purely conceptual alignment model.

Table 5. Computational Feasibility.

Solver	Runtime
Greedy heuristic	0.8 s
Integer optimization	3.4 s

Residual enterprise risk as a function of digital interdependence level (κ) comparing Governance-Constrained Cyber Risk Optimization Method (GCCROM) with baseline governance and ERM-based decision models. As enterprise interconnection increases, conventional approaches exhibit near-linear risk escalation, whereas GCCROM maintains bounded residual risk due to dependency-aware control allocation.

Figure 2 illustrates how enterprise risk evolves when the degree of digital interdependence increases. In low-coupling environments all models exhibit similar behaviour because risks remain largely localized. However, as interdependence grows, the baseline governance model and ERM scoring model show steady risk amplification. This occurs because both approaches prioritize direct asset exposure and do not explicitly account for cascading propagation across connected services. By contrast, the proposed GCCROM demonstrates a significantly slower increase in residual risk. The curve remains nearly bounded even at high interdependence levels. The behaviour emerges because the optimization process reallocates controls toward shared infrastructure and propagation-critical nodes rather than isolated endpoints. Consequently, the model suppresses secondary risk amplification instead of reacting only to primary vulnerabilities. Rather than minimizing independent risks, the proposed framework minimizes network-level exposure. This confirms that the method adapts to enterprise architecture complexity and supports resilient decision-making in highly integrated digital environments.

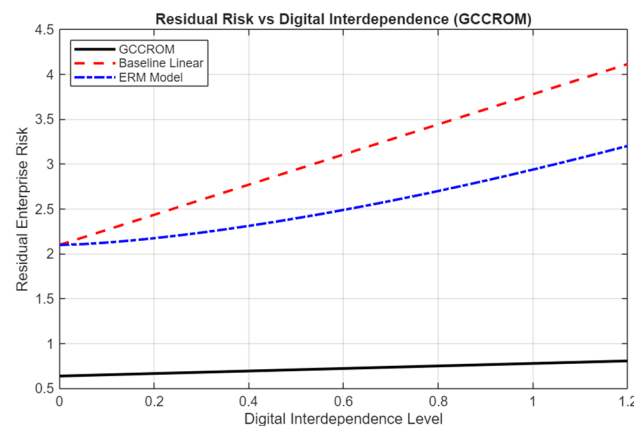


Figure 2. Residual Enterprise Risk under Increasing Digital Interdependence.

7. Conclusions and Future Directions

7.1. Conclusions

This study addressed the growing challenge of aligning digital governance, enterprise risk management, and cybersecurity decision-making in increasingly complex enterprise environments. Through a critical examination of existing governance-centric, ERM-integrated, and operational cybersecurity approaches, it was observed that prevailing models often operate in silos, resulting in misalignment between strategic intent and cybersecurity execution.

To overcome this limitation, the paper proposed the Governance-Constrained Cyber Risk Optimization Method (GCCROM), which formalizes cybersecurity governance as a constrained decision-making problem. By embedding governance parameters—such as risk appetite, policy boundaries, budgetary limits, and operational tolerance—directly into the cybersecurity optimization process, the proposed method ensures that security decisions are both risk-aware and governance-compliant by design. The incorporation of multidimensional risk decomposition and nonlinear digital interdependence modelling further enables early detection of cascading risk behaviours that are insufficiently captured by conventional linear or qualitative models.

The analytical comparison and illustrative numerical scenario demonstrated that GCCROM offers measurable advantages over commonly adopted approaches in terms of risk sensitivity, control allocation efficiency, governance alignment, and adaptability. These results confirm that the proposed methodology extends beyond conceptual alignment frameworks by providing a structured, decision-oriented mechanism capable of supporting consistent and proactive cybersecurity governance in digitally intensive enterprises.

7.2. Implications for Practice

From a practical perspective, the proposed method provides enterprise leaders, risk managers, and cybersecurity teams with a common decision framework that bridges strategic governance and operational execution. By translating governance intent into quantifiable constraints and optimization objectives, the model improves transparency, accountability, and coordination across organizational functions. Additionally, the method supports more efficient cybersecurity investment decisions under resource constraints, which is particularly relevant for large, distributed, and digitally interconnected enterprises.

The framework also offers value in regulatory and audit contexts by enabling organizations to demonstrate continuous, governance-aligned risk management rather than static compliance adherence. This capability aligns with emerging regulatory expectations that emphasize cyber resilience and accountability.

7.3. Limitations and Future Directions

While the proposed methodology provides a strong analytical foundation, this study has certain limitations. The comparative evaluation is model-driven and illustrative in nature, rather than empirically validated using real-world enterprise datasets. This limitation reflects the practical challenges associated with accessing sensitive cybersecurity data but also highlights opportunities for future research.

Future work may focus on empirical validation of the model using anonymized organizational data or industry-specific case studies. Simulation-based experiments could further explore the sensitivity of the optimization outcomes to changes in governance parameters, digital interdependence levels, and threat dynamics. Additionally, the integration of predictive analytics and automated decision-support mechanisms could enhance the adaptability and scalability of the proposed approach. Sector-specific extensions of the framework—for

domains such as finance, healthcare, and critical infrastructure—also represent promising avenues for future investigation.

7.4. Final Remarks

Overall, this work contributes a novel, analytically grounded approach to enterprise cybersecurity governance by unifying governance intent, enterprise risk dynamics, and cybersecurity execution within a single optimization framework. By reframing cybersecurity governance as a constrained and adaptive decision process, the proposed method offers a practical pathway for strengthening digital resilience and governance effectiveness in complex enterprise environments.

Author Contributions: Conceptualization, K.K.J. and K.S.; methodology, K.K.J.; software, K.K.J.; validation, K.K.J. and K.S.; formal analysis, K.K.J.; investigation, K.K.J. and K.S.; resources, K.K.J.; data curation, K.K.J.; writing—original draft preparation, K.K.J.; writing—review and editing, K.K.J. and K.S.; visualization, K.K.J.; supervision, K.K.J.; project administration, K.K.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new datasets were generated or analyzed during the current study. The study is based on analytical modelling, simulation, and publicly available literature. Data supporting the findings are available from the corresponding author upon reasonable request.

Acknowledgments: The authors would like to acknowledge the academic and institutional support that contributed to the completion of this research. The authors also thank colleagues and peers for their constructive discussions and feedback, which helped improve the clarity and quality of this work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Larcker, D.F.; Reiss, P.C.; Tayan, B. *Critical Update Needed: Cybersecurity Expertise in the Boardroom*; Stanford Closer Look Series No. CGRP-69; Stanford University Graduate School of Business Research Paper No. 17-70; Corporate Governance Research Initiative, Stanford Graduate School of Business: Stanford, CA, USA, 2017. Available online: <https://www.gsb.stanford.edu/faculty-research/publications/critical-update-needed-cybersecurity-expertise-boardroom> (accessed on 10 August 2026).
2. Romanosky, S.; Petrun Sayers, E.L. Enterprise risk management: How do firms integrate cyber risk? *Manag. Res. Rev.* **2024**, *47*, 1–17. [CrossRef]
3. Abdul-Azeez, O.; Ihechere, A.O.; Idemudia, C. Digital access and inclusion for SMEs in the financial services industry through cybersecurity GRC: A pathway to safer digital ecosystems. *Financ. Account. Res. J.* **2024**, *6*, 1134–1156. [CrossRef]
4. Nodehi, S.; Huygh, T.; Bollen, L. Six board roles for information security governance. In Proceedings of the International Conference on Information Systems Security and Privacy, Angers, France, 28–30 April 2024; pp. 713–720. [CrossRef]
5. Setiawan, A.; Mufti, A.; Mau, F.A.; Purkoni, A.; Setiawan, A. Bridging cybersecurity and enterprise risk management in the digital era. *TechComp Innov. J. Comput. Sci. Technol.* **2025**, *2*, 28–38. [CrossRef]
6. Gorbanova, V.; Gorbanov, I. International experience in corporate management of cybersecurity enterprises. *Her. UNU Int. Econ. Relat. World Econ.* **2025**, *57*, 713–720. [CrossRef]
7. Metin, B.; Özhan, F.G.; Wynn, M. Digitalisation and Cybersecurity: Towards an Operational Framework. *Electronics* **2024**, *13*, 4226. [CrossRef]
8. Olatunde-Thorpe, J.; Aifuwa, S.E.; Oshoba, T.; Ogbuefi, E.; Akokodariapon, D. Framework for aligning organizational risk culture with cybersecurity governance objectives. *Int. J. Multidiscip. Futur. Dev.* **2021**, *2*, 61–71. [CrossRef]
9. Panabergenova, J.; Umarova, K. Corporate governance cybersecurity framework in CIS countries: Comparative analysis of regulatory standards and digital risk management practices. *Int. Cybersecur. Law Rev.* **2025**, *6*, 367–376. [CrossRef]

10. Thuraisingham, B. Cyber Security and Data Governance Roles and Responsibilities at the C-Level and the Board. In *Proceedings of the 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, 1–3 July 2019*; IEEE: Piscataway, NJ, USA, 2019; pp. 231–236. [[CrossRef](#)]
11. Thapaliya, S.; Panta, S. Cybersecurity Decision-Making in the C-Suite: A Framework for Managerial Engagement. *J. Eng. Issues Solut.* **2025**, *4*, 111–120. [[CrossRef](#)]
12. Zaydi, M.; Nassereddine, B. A New Comprehensive Solution to Handle Information Security Governance in Organizations. In *Proceedings of the 2nd International Conference on Networking, Information Systems & Security (NISS 2019), Rabat, Morocco, 27–29 March 2019*; ACM: New York, NY, USA, 2019; pp. 1–5. [[CrossRef](#)]
13. Suresh, M.N.; Varalakshmi, T.; Chand, M.S. IT Governance Framework Ensuring Effective Management and Compliance. *Int. Res. J. Adv. Eng. Manag.* **2024**, *2*, 1627–1632. [[CrossRef](#)]
14. Ajayi, J.O.; Cadet, E.; Essien, I.A.; Erigha, E.D.; Obuse, E.; Ayanbode, N.; Babatunde, L.A. Building Resilient Enterprise Risk Programs through Integrated Digital Governance Models. *Int. J. Sci. Res. Humanit. Soc. Sci.* **2024**, *1*, 433–462. [[CrossRef](#)]
15. Oluoha, O.; Odeshina, A.; Reis, O.; Okpeke, F.; Attipoe, V.; Orieno, O.H. Project management innovations for strengthening cybersecurity compliance across complex enterprises. *Int. J. Multidiscip. Res. Growth Eval.* **2021**, *2*, 871–881. [[CrossRef](#)]
16. Kekgathetse, M.; Lucas, B.; Sebapalo, M. A Systematic Review on Cyber Security Integration in Information Technology Governance. In *Proceedings of the 2024 International Conference on Electrical and Computer Engineering Researches (ICECER), Gaborone, Botswana, 4–6 December 2024*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–6. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.