International Journal of Multidisciplinary Research and Growth Evaluation
ISSN: 2582-7138
Received: 20-11-2020; Accepted: 22-12-2020
www.allmultidisciplinaryjournal.com
Volume 1; Issue 5; November-December 2020; Page No. 984-991

A Quantitative Cyber Risk Valuation Model for Board-Level Decision Making in Critical Infrastructure

Beloved D Smart SSCP
Manager CyberSecurity Governance, Risk and Compliance, Multinational Technologies Ltd, Lagos, Nigeria

Corresponding Author: **Beloved D Smart SSCP**

DOI: https://doi.org/10.54660/.IJMRGE.2020.1.5.984-991

Abstract
Critical infrastructure organizations face a growing gap between the sophistication of cybersecurity threats and the ability of governance frameworks to translate that risk into financially grounded intelligence for board-level decisions. This gap reflects not a lack of technical risk data but a failure to translate threat intelligence and vulnerability information into monetary probabilistic expressions that boards need to oversee cybersecurity investment alongside other enterprise risks. This paper proposes a Quantitative Cyber Risk Valuation model. It integrates Factor Analysis of Information Risk's probabilistic decomposition Gordon-Loeb investment optimization and the NIST Risk Management Framework. The model is structured for governance output and is intended for critical infrastructure operators in energy water financial services transportation and healthcare. The model produces probability-weighted annual loss expectancies specified at tenth fiftieth and ninetieth percentile confidence intervals. It also provides an investment efficiency frontier so organizations can identify security allocations that maximize risk reduction per capital unit in line with Gordon-Loeb optimality. Furthermore it provides a structured risk appetite framework that helps boards define enforce and monitor quantitative risk thresholds aligned with risk tolerance and regulatory requirements. The paper reviews the literature on security economics quantitative risk board governance industrial control system security and enterprise IT frameworks to develop a model applicable to regulated organizations across sectors and jurisdictions

Keywords: cyber risk quantification, board governance, FAIR methodology, critical infrastructure, annualized loss expectancy, risk appetite, NIST RMF, Monte Carlo simulation, Gordon-Loeb, investment optimization

1. Introduction
The primary cybersecurity governance challenge for boards of critical infrastructure organizations is a translation issue between technical risk outputs and the financial terminology required for board-level decision-making. Security practitioners typically employ technical risk analysis terms such as vulnerability severity ratings threat actor capability assessments control maturity scores and attack surface characterizations. These technical metrics do not directly correspond to the financial and strategic language boards use to assess organizational risk and allocate capital. Consequently, a persistent misalignment exists between authorized security investments and the actual risk reduction achieved particularly when boards base security budgets on qualitative risk narratives rather than rigorous financial analysis of expected loss reduction per dollar invested [7, 8, 9, 10]. The QCRV model addresses this governance gap by providing a methodological translation layer that generates financially expressed risk intelligence tailored for board deliberation on investment allocation and risk appetite.

The consequences of inadequate board-level cybersecurity oversight in critical infrastructure organizations extend beyond financial loss to encompass national economic stability public health and physical safety. For example, ransomware attacks on hospital networks can disrupt clinical care and directly increase patient mortality as interruptions in electronic medical record access have well-documented safety implications. Similarly, successful attacks on electric grid supervisory control systems can cause cascading failures affecting millions of individuals and resulting in economic losses that may reach billions of dollars per day in densely populated areas. Supply chain intrusions in the defense sector can compromise programs with geopolitical significance. The scale of these risks imposes a governance responsibility on boards of critical infrastructure organizations to provide substantive and informed oversight a responsibility that cannot be fulfilled by ordinal risk categorization systems currently prevalent in security reporting [8, 9, 17, 18, 31].

ate directors lack the technical background to critically evaluate security reports. Ordinal risk rating systems labeling risk as high medium or low on color-coded heat maps do not provide a sound basis for the financial comparisons boards use to allocate capital. When security teams report ransomware risk as high boards cannot determine whether this means expected annual losses of $5 million or $500 million. They cannot know if a two-million-dollar investment will materially reduce the risk or only marginally address it or whether it is financially rational to accept the risk level given risk capacity and strategic objectives. The same board when evaluating a capital investment uses net present value analysis examines probability distributions of returns and compares risk-adjusted returns with other capital uses. This is the kind of financially rigorous analysis the QCRV model brings to cybersecurity decisions [8, 9, 17, 18].

The QCRV model addresses both the measurement and translation aspects of board governance challenges through a four-layer architecture. The Data Ingestion and Asset Valuation layer quantifies the monetary value of assets at risk across technological and operational domains. The Threat Intelligence and Scenario Construction layer models adversary capabilities and attack pathways using structured intelligence. The Quantitative Risk Engine employs the FAIR probabilistic methodology and Monte Carlo simulation to generate financial loss distributions for individual scenarios and in aggregate. The Board Governance Output Layer presents risk results in four formats tailored for board deliberation on investment allocation risk appetite and regulatory compliance. This architecture is calibrated with sector-specific packages for five critical infrastructure sectors integrating threat profiles regulatory penalty schedules and operational disruption loss models relevant to each sector's risk environment [1, 2, 3, 4, 12].

The development of the QCRV model builds upon prior conceptual frameworks including the insider threat classification and risk modeling taxonomy [33] the risk-based cybersecurity assurance framework [34] and the privacy-focused security engineering model [35]. These foundational works inform the QCRV model's scenario library parameterization methods and governance integration. Additionally, research on digital literacy and responsible technology education [32] guides the board capacity development component of the QCRV implementation.

2. Methodology

This paper adopts a methodology for conceptual framework development that combines a structured literature review with deductive framework synthesis. The research design follows the established tradition of conceptual modeling in information security governance research wherein theoretical frameworks are constructed by synthesizing principles from economics risk management and regulatory science rather than through primary empirical data collection. The methodological approach is appropriate to the research objective: developing a governance model to structure board-level deliberation rather than reporting findings from organizational experiments.

A structured review of the academic literature was conducted using Google Scholar the ACM Digital Library IEEE Xplore and Scopus. Search terms included: cyber risk quantification board governance cybersecurity FAIR methodology annualized loss expectancy critical infrastructure security Gordon-Loeb investment optimization information security economics and risk appetite framework. The review timeframe prioritized publications from 2000 to 2020 with foundational pre-2000 works incorporated where their contributions remain the theoretical basis of current practice. Government publications regulatory documents and international standards from NIST ISO ISACA and sector-specific regulatory bodies were included due to their authoritative status in the governance domain.

Source selection applied inclusion criteria requiring that publications address at least one of the following: quantitative risk measurement methodology for cybersecurity board-level governance of technology or security risk critical infrastructure security management investment optimization under uncertainty or NIST Risk Management Framework governance processes. Sources were excluded if they addressed technical security topics without governance implications were superseded by subsequent authoritative editions or were opinion pieces without methodological grounding. Practitioner consultation with senior enterprise architecture and banking operations executives provided practitioner validation confirming that the framework components reflect operational governance realities experienced in complex regulated financial institutions.

The framework development process proceeded through three stages. In the first stage theoretical principles from security economics quantitative risk management and board governance research were synthesized into a set of design requirements that any adequate board-level cyber risk governance model must satisfy. In the second stage existing quantitative risk frameworks — specifically FAIR NIST SP 800-30 and Gordon-Loeb optimization — were evaluated against these design requirements and selected as foundation components whose integration would satisfy requirements not fully addressed by any individual framework. In the third stage the integrated model's architecture was evaluated against the design requirements and refined through iterative evaluation until theoretical consistency and practical deplorability were satisfactorily established.

3. Theoretical Foundations

3.1. Economics of Information Security Investment

The theoretical foundation for the QCRV model's investment optimization component rests on Gordon and Loeb's demonstration that the economically optimal level of security investment for a rational organization can be analytically derived from two parameters: the probability of a security breach in the absence of additional measures and the potential financial loss associated with that breach [2]. The model's central result that optimal investment is bound above at approximately 37% of potential breach loss regardless of breach probability establishes both an upper bound for investment efficiency analysis and a theoretical anchor for the QCRV Investment Efficiency Frontier. This result is counterintuitive relative to the prevailing compliance-driven investment approach where organizations may invest substantially more than this bound if frameworks prescribe comprehensive controls without calibration to actual loss exposure. Extensions of the Gordon-Loeb framework document the economic value of information sharing in cybersecurity markets providing theoretical justification for threat intelligence programs as prerequisites for accurate scenario parameterization [11].

Hubbard and Seiersen's methodological work validate that

calibrated probability estimation by domain experts structured through formal analytical decomposition and validated through simulation produces risk estimates that are significantly superior to the ordinal qualitative categorizations that dominate enterprise risk practice [7]. Their demonstration that decomposing complex risk questions into simpler independently estimable sub-questions precisely the decomposition structure provided by FAIR substantially improves estimation accuracy resolving the frequently raised objection that cybersecurity risk cannot be meaningfully quantified due to data scarcity. Calibrated expert estimation supplemented by industry benchmark data yields financial risk estimates whose reliability substantially exceeds that of qualitative assessments that organizations currently produce with equivalent human resources. Anderson and Moore's analysis of information security economics documents systematic market failures that justify regulatory intervention and create the regulatory accountability context within which the QCRV model's Regulatory Exposure Tracker operates [9, 10].

ISO 31000's risk management principles establish risk appetite as a foundational governance construct that should be quantitatively defined formally approved by the board and operationalized through risk limits and monitoring thresholds triggering governance action when exceeded [37, 46]. COBIT 5 provides the IT governance framework within which the QCRV model's data collection and evidence management architecture operates establishing the accountability linkages between IT management activities and board-level governance reporting [38, 47]. The CIS Controls Version 7.1 published in 2019 provides a prioritized security control framework whose risk-reduction ordering logic parallels the QCRV model's Investment Efficiency Report confirming that the broader security governance community has independently converged on risk-prioritized investment frameworks as the appropriate basis for security program design [14]. General information security management principles established in foundational security engineering texts and Principles of Information Security provide the conceptual vocabulary within which QCRV model outputs are interpreted and communicated to board members with varying levels of technical background [48, 49].

3.2. Fair Methodology and Risk Decomposition

The Factor Analysis of Information Risk methodology provides the analytical decomposition framework through which the QCRV model converts technical risk information into financial risk distributions. FAIR decomposes risk into two analytically independent primary components: Loss Event Frequency which characterizes how often a loss event is expected to occur and Loss Magnitude which characterizes the financial impact when it occurs. Each is further decomposed into independently estimable sub-components: Threat Event Frequency and Vulnerability for LEF; Productivity Response Replacement Competitive Advantage Fines and Judgments and Reputation for LM enabling domain experts to estimate complex aggregate risk scenarios by answering simpler analytical questions whose difficulty matches their expertise [1]. The FAIR decomposition makes risk estimates interrogatable by board members without deep technical expertise: a board examining a ransomware loss estimate can evaluate the plausibility of individual component estimates using institutional knowledge of operations and regulatory exposure rather than accepting an opaque aggregate figure.

NIST SP 800-30 Rev. 1 provides the authoritative federal guidance on information security risk assessment establishing the vocabulary and assessment structure within which the QCRV model operates [3]. NIST SP 800-39 establishes a three-tier organizational risk management architecture positioning QCRV outputs as organizational-tier intelligence that informs governance decisions and cascades through lower tiers [4]. NIST SP 800-37 Rev. 2 establishes the Risk Management Framework cycle providing the process structure within which QCRV's continuous update architecture operates at the organizational tier ensuring board-level risk governance remains synchronized with the underlying security assessment cycle [12]. NIST SP 800-53 Rev. 5 published in September 2020 provides the comprehensive security control catalog from which the Investment Efficiency Report's risk treatment options are drawn ensuring recommended investments map to the established control framework that most regulated organizations' security programs already reference [4].

3.3. Board Governance Theory

Srinidhi Yan and Bhargava establish a positive association between information security investment levels and the intensity of board-level oversight particularly when directors have relevant technical expertise and when cybersecurity is a standing board agenda item [8]. Higgs Pinsker Smith and Young document that organizations with board-level technology governance committees experienced materially lower breach rates confirming that governance structure influences security outcomes [9]. The ISO/IEC 27001:2013 standard establishes the information security management system framework within which the QCRV model's continuous risk monitoring architecture operates for organizations seeking internationally recognized certification of their security governance program [36, 47]. Prior conceptual work on insider threat classification and risk modeling provides an adversary behavior taxonomy for QCRV scenarios targeting internally sourced risks recognizing that insider threats are systematically underweighted by intelligence-driven scenario approaches that primarily focus on external adversaries [33].

4. The Qcrv Model Architecture

4.1. Design Principles

The QCRV model is organized around five design principles. The Financial Expressibility Principle requires all risk outputs to be expressed in monetary terms and directly comparable to the financial metrics boards use to evaluate other enterprise risks. The Probabilistic Uncertainty Principle requires outputs to explicitly represent estimation uncertainty enabling boards to distinguish between scenarios where additional analysis would usefully narrow confidence intervals and scenarios where fundamental uncertainty warrants conservative risk capacity management rather than precision-seeking analytical investment. The Governance Utility Principle requires that every output be designed to support a specific board of governance decision. The Calibration Transparency Principle requires that model parameters be documented with data sources uncertainty representations and update histories enabling boards to interrogate the analytical basis of estimates. The Sector Specificity Principle requires all calibration to reflect the specific characteristics of the organization's critical

infrastructure sector. Enterprise architecture practitioners in regulated banking contexts confirm that sector-specificity is the most important design element for building board confidence in risk governance frameworks.

4.2. Asset Valuation and Threat Intelligence Layers

The Asset Valuation layer constructs a comprehensive financial representation of assets at risk across technology and operational environments drawing on configuration management databases OT asset inventories cloud management platforms and human capital systems. Each asset is assigned three monetary characterizations that extend NIST SP 800-30's asset classification framework incorporating critical infrastructure dimensions: Operational Criticality (the financial cost of operational disruption) Regulatory Consequence (penalty exposure from compromise) and Public Safety Impact (the potential for physical harm). Asset valuations are derived through four-method triangulation combining replacement cost analysis revenue contribution attribution regulatory penalty schedule review and operational disruption cost modeling. The NIST SP 800-82 Rev. 2 guidance on industrial control system security provides the technical framework reference for OT asset characterization in energy and water sector implementations [20, 3, 4].

Threat intelligence is ingested from sector ISACs government advisories commercial intelligence platforms and open-source reporting normalized using standard exchange formats and mapped to the MITRE ATT&CK framework taxonomy current at the time of model development. Scenarios are constructed by pairing threat actor profiles from the Threat Actor Catalog with asset classes thereby generating structured specifications that define an adversary attack pathway target asset and consequence chain. FAIR parameter distributions for each scenario are estimated through structured expert elicitation using calibrated probability estimation with each parameter characterized by a minimum most-likely and maximum range fitted to a PERT distribution to enable Monte Carlo sampling. The INDUSTROYER and TRISIS campaigns whose technical analyses were publicly available by 2020 confirm the adversary's capability to develop OT protocol-specific attack tools informing the high-severity end of OT-targeted scenario libraries for energy and chemical-sector implementations [41, 42].

4.3. Quantitative Risk Engine and Board Outputs

The Risk Engine executes probabilistic simulations across the full prioritized scenario library sampling from FAIR parameter distributions and iterating until convergence in the distribution tails critical for risk capacity analysis. Aggregate organizational risk is computed using a Gaussian copula correlation structure preventing both overestimation from assuming full positive correlation and underestimation from assuming complete independence. Gordon-Loeb investment efficiency optimization is applied as a post-simulation layer computing the marginal risk reduction achievable from each proposed security investment by re-running the simulation with the proposed control's effects on affected scenario parameters and computing the change in aggregate expected annual loss. The Investment Efficiency Ratio of marginal ALE reduction to investment cost enables board comparison of security investments on the same financial efficiency terms as other capital expenditures [2, 7].

The Bayesian parameter update mechanism enables accuracy improvement as organizational experience accumulates. At initialization parameters are drawn from sector-level prior distributions. As the organization experiences incidents near-misses and assessments posterior distributions are updated using Bayesian inference progressively narrowing uncertainty ranges. Organizations sustaining the QCRV model over multiple years develop increasingly accurate estimates reflecting their specific threat environment and control effectiveness creating compounding governance value. The COBIT 5 framework provides the governance accountability structure through which Bayesian update data flows from operational security activities to governance reporting [38, 47].

The four Board Governance Output Views address the board deliberation decisions that security reporting most consequentially influences. The Executive Risk Summary presents aggregate risk as a financial distribution compared against Risk Appetite thresholds with trend indicators. The Scenario Heat Map plots priority scenarios on probability and magnitude axes enabling boards to distinguish near-term investment priorities from risk transfer candidates. The Investment Efficiency Report presents proposed investments ranked by IER on the Gordon-Loeb efficient frontier. The Regulatory Exposure Tracker maps scenarios to applicable regulatory frameworks and quantifies financial penalty exposure. ISO 31000's risk reporting principles inform the format and content of all four views ensuring compatibility with enterprise-wide risk governance communication standards [37].

4.4. Risk Appetite Framework

The QCRV Risk Appetite Framework operationalizes the enterprise risk management risk appetite construct into quantitatively defined continuously monitored governance constraints. The framework distinguishes Risk Capacity (the objective boundary below which the organization can absorb loss without threatening viability) Risk Appetite (the deliberate preference boundary within capacity) and Risk Tolerance (the operational early-warning threshold that triggers proactive management before appetite is reached). All three are expressed in financial terms enabling precise definition continuous monitoring and threshold-triggered escalation. When the Risk Engine detects aggregate risk exceeding the Risk Tolerance threshold the framework generates a structured Decision Package for board consideration that includes driving scenario characterization; quantified current risk with a confidence interval; three to five risk treatment options with IERs; recommended treatment with rationale; implementation timeline; and projected residual risk. ISO 31000's risk treatment and communication framework provides the process reference for the Decision Package structure and board engagement protocol [37, 46].

5. Sector Calibration and Implementation

Financial services sector calibration incorporates banking regulatory penalty schedules from OCC Federal Reserve FDIC and FinCEN enforcement data; threat scenarios emphasizing account takeover payment fraud and ransomware campaigns; and loss magnitude parameterization drawing on 2019 industry data breach cost studies demonstrating median breach costs in the multi-million-dollar range for financial institutions [22, 23, 24]. Energy sector calibration incorporates NERC CIP penalty structures

NIST SP 800-82 Rev. 2 OT security framework requirements and operational disruption loss models. Water sector calibration reflects SCADA attack patterns from 2013-2019 public reporting EPA penalty schedules and public safety consequence characterizations for scenarios involving physical disruption of treatment processes. Implementation follows four phases over 19 months from baseline asset valuation through full continuous governance operation with the COBIT 5 IT governance framework providing the organizational accountability structure for each implementation phase [20, 38].

6. Conceptual Analysis and Limitations

The QCRV model's most significant theoretical contribution is its resolution of the translation failure between cybersecurity risk practice and board governance by producing governance-native financial outputs rather than technical outputs that require secondary translation. Prior approaches to improving board cybersecurity governance focused on the communication dimension improving vocabulary and presentation quality without addressing the underlying measurement dimension. The QCRV model addresses both simultaneously: FAIR produces intrinsically board-comprehensible financial risk metrics and the structured output architecture presents those metrics in formats aligned with the governance decisions boards regularly face. The investment efficiency framework establishes a theoretically grounded basis for determining when additional security investment generates positive expected value a determination currently made almost universally without formal economic analysis [2, 8, 9, 10].

Limitations include reliance on organizational data quality for parameter estimation which creates systematic limitations for organizations at early maturity stages with incomplete asset inventories. The Monte Carlo methodology assumes distributional forms that may inadequately characterize heavy-tailed catastrophic cyber-loss events; future research should integrate extreme-value theory with Monte Carlo simulation. The CIS Controls Version 7.1 risk-prioritized sequencing logic provides a validation reference for the QCRV Investment Efficiency Report's recommended control sequencing confirming that multiple independent frameworks have converged on risk-prioritized investment as the appropriate security program design principle [14]. The ENISA 2019 threat landscape report provides macro-level context for the threat environment in which specific QCRV scenarios are situated for EU-operating critical infrastructure organizations [55].

The governance integration architecture of the QCRV model connects quantitative risk outputs to three specific board governance processes that existing risk reporting architectures do not adequately support. Investment allocation governance uses the Investment Efficiency Report to enable boards to evaluate security budget proposals against a common standard of risk-reduction efficiency selecting among alternatives on the basis of annualized loss reduction per dollar invested rather than qualitative risk narrative. Risk appetite governance uses the Risk Appetite Framework to enable boards to formally adopt quantitative risk thresholds specifying for example that the organization will maintain an expected annual loss at the 90th percentile below a defined monetary threshold across all critical infrastructure scenarios and to continuously monitor compliance with those thresholds through the Executive Risk Dashboard. Regulatory accountability governance uses the Regulatory Exposure Tracker to maintain real-time visibility into the organization's exposure to regulatory penalties from identified control gaps enabling boards to discharge their oversight responsibilities over regulatory compliance with financial precision rather than categorical judgment [8, 9].

The QCRV model's sector calibration architecture reflects the fundamental diversity of critical infrastructure operational risk environments. Energy-sector implementations must account for the kinetic consequences of electric grid disruption including potential grid instability load-shedding cascades and extended restoration timelines affecting industrial customers dependent on reliable power using operational disruption loss models that extend well beyond the customer-revenue-loss framework adequate for commercial-sector disruptions. Water sector implementations must incorporate public health consequence modeling to address the health and liability costs of compromised treatment or distribution systems including the potential for mass casualty events in extreme scenarios involving safety system compromise analogous to the TRISIS threat model [23, 24, 25]. Financial services sector implementations must address contagion risk the potential for a single organization's compromise to trigger systemic instability through correspondent banking relationships payment system interconnections and clearinghouse dependencies which is largely absent from other critical infrastructure sectors but poses the most complex board governance challenge.

The QCRV model's quantitative foundation enables a governance capability that qualitative frameworks cannot support: continuous monitoring of compliance with board-approved risk appetite thresholds with automatic escalation triggers when updated threat intelligence or newly identified vulnerabilities cause risk estimates to exceed approved thresholds between scheduled board reporting cycles. This continuous monitoring capability transforms the risk appetite framework from a statement of intent into an operationally enforced governance constraint analogous to the real-time limit-monitoring frameworks financial institutions have used for market and credit risk for decades. The adaptation of financial risk management monitoring practices to cybersecurity risk governance is theoretically sound as both domains address expected losses from uncertain adverse events and are practically valuable as boards with financial services experience already understand the governance logic of monitored risk thresholds [8, 2, 7].

Implementation of the QCRV model requires organizational investment in three capability areas that many critical infrastructure organizations currently lack. First financial analysis capability within the information security function to support FAIR parameter estimation Monte Carlo execution and board-quality output preparation a capability distinct from technical security analysis and requiring hybrid expertise in both financial modeling and security risk assessment. Second executive and board education to develop sufficient quantitative risk literacy so board members can critically evaluate probabilistic risk outputs rather than passively accept practitioner representations of their meaning. Third the institutional data infrastructure captures asset valuation loss events and control effectiveness data thereby improving the accuracy of parameter estimation across successive model update cycles. These capability investments are themselves amenable to QCRV analysis

enabling a model-informed business case for the investment required to operate the model effectively [7, 32].

The governance integration architecture of the QCRV model connects quantitative risk outputs to three specific board governance processes that existing risk reporting architectures do not adequately support. Investment allocation governance uses the Investment Efficiency Report to enable boards to evaluate security budget proposals against a common standard of risk-reduction efficiency selecting among alternatives on the basis of annualized loss reduction per dollar invested rather than qualitative risk narrative. Risk appetite governance uses the Risk Appetite Framework to enable boards to formally adopt quantitative risk thresholds specifying for example that the organization will maintain an expected annual loss at the 90th percentile below a defined monetary threshold across all critical infrastructure scenarios — and to continuously monitor compliance with those thresholds through the Executive Risk Dashboard. Regulatory accountability governance uses the Regulatory Exposure Tracker to maintain real-time visibility into the organization's exposure to regulatory penalties from identified control gaps enabling boards to discharge their oversight responsibilities over regulatory compliance with financial precision rather than categorical judgment [8, 9].

The QCRV model's sector calibration architecture reflects the fundamental diversity of critical infrastructure operational risk environments. Energy-sector implementations must account for the kinetic consequences of electric grid disruption including potential grid instability load-shedding cascades and extended restoration timelines affecting industrial customers dependent on reliable power using operational disruption loss models that extend well beyond the customer-revenue-loss framework adequate for commercial-sector disruptions. Water sector implementations must incorporate public health consequence modeling to address the health and liability costs of compromised treatment or distribution systems including the potential for mass casualty events in extreme scenarios involving safety system compromise analogous to the TRISIS threat model [23, 24, 25]. Financial services sector implementations must address contagion risk the potential for a single organization's compromise to trigger systemic instability through correspondent banking relationships payment system interconnections and clearinghouse dependencies which is largely absent from other critical infrastructure sectors but poses the most complex board governance challenge.

The QCRV model's quantitative foundation enables a governance capability that qualitative frameworks cannot support: continuous monitoring of compliance with board-approved risk appetite thresholds with automatic escalation triggers when updated threat intelligence or newly identified vulnerabilities cause risk estimates to exceed approved thresholds between scheduled board reporting cycles. This continuous monitoring capability transforms the risk appetite framework from a statement of intent into an operationally enforced governance constraint analogous to the real-time limit-monitoring frameworks financial institutions have used for market and credit risk for decades. The adaptation of financial risk management monitoring practices to cybersecurity risk governance is theoretically sound as both domains address expected losses from uncertain adverse events and is also practically valuable as boards with financial services experience already understand the governance logic of monitored risk thresholds [8, 2, 7].

Implementation of the QCRV model requires organizational investment in three capability areas that many critical infrastructure organizations currently lack. First financial analysis capability within the information security function to support FAIR parameter estimation Monte Carlo execution and board-quality output preparation a capability distinct from technical security analysis and requiring hybrid expertise in both financial modeling and security risk assessment. Second executive and board education to develop sufficient quantitative risk literacy so board members can critically evaluate probabilistic risk outputs rather than passively accept practitioner representations of their meaning. Third the institutional data infrastructure captures asset valuation loss events and control effectiveness data thereby improving the accuracy of parameter estimation across successive model update cycles. These capability investments are themselves amenable to QCRV analysis enabling a model-informed business case for the investment required to operate the model effectively [7, 32].

7. Conclusion

The QCRV model provides critical infrastructure boards with a financially rigorous board-comprehensible framework for quantifying cybersecurity risk and making investment decisions. By integrating FAIR quantification Gordon-Loeb investment optimization NIST RMF governance architecture and a structured board output layer calibrated for deliberation on critical infrastructure the model enables substantive financially grounded oversight at the governance level where it produces the greatest organizational and societal impact. Development builds on security economics theory quantitative risk measurement board governance research enterprise IT governance standards prior conceptual work on insider threat classification risk-based assurance privacy-centric security engineering and digital literacy education providing a theoretically grounded and practically deployable governance solution for the board-level cybersecurity oversight challenge facing critical infrastructure organizations.

Data-driven risk evaluation models for emerging-market financial institutions provide methodological precedents for the calibrated estimation approach that the QCRV model applies to critical infrastructure loss scenarios demonstrating that probabilistic risk assessment under data scarcity is achievable through structured decomposition and expert elicitation [57]. Technology-enabled internal audit quality research shows that integrating a risk assessment framework significantly improves the quality and coverage of organizational risk identification supporting the QCRV model's integration of multiple risk identification methodologies into a unified board-governance architecture [58]. Risk-based internal control frameworks for banking and insurance confirm that quantitative risk calibration produces governance architectures that are substantially more effective than compliance-oriented control models at achieving the risk-reduction objectives that boards authorize investments to accomplish [59, 60].

References

1. The Open Group. Open FAIR: Factor analysis of information risk—body of knowledge. The Open Group Standard; 2013.
2. Gordon LA Loeb MP. The economics of information security investment. ACM Trans Inf Syst Secur. 2002;5(4):438–457.
3. National Institute of Standards and Technology. Guide for conducting risk assessments. NIST SP 800-30 Rev. 1; 2012.
4. National Institute of Standards and Technology. Managing information security risk. NIST SP 800-39; 2011.
5. National Institute of Standards and Technology. Security and privacy controls for information systems and organizations. NIST SP 800-53 Rev. 5; 2020.
6. Anderson R Moore T. The economics of information security. Science. 2006;314(5799):610–613.
7. Hubbard DW Seiersen R. How to measure anything in cybersecurity risk. Hoboken (NJ): Wiley; 2016.
8. Higgs JL Pinsker RE Smith TJ Young GR. The relationship between board-level technology committees and reported security breaches. J Inf Syst. 2016;30(3):79–98.
9. Srinidhi B Yan J Bhargava HK. Effect of information security investments on firm performance. Decis Support Syst. 2015;74:1–15.
10. Gordon LA Loeb MP Lucyshyn W. Sharing information on computer systems security: An economic analysis. J Account Public Policy. 2003;22(6):461–485.
11. National Institute of Standards and Technology. Risk management framework for information systems and organizations. NIST SP 800-37 Rev. 2; 2018.
12. Presidential Policy Directive 21—Critical infrastructure security and resilience; 2013.
13. National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity. Version 1.1; 2018.
14. Center for Internet Security. CIS controls version 7.1; 2019.
15. Verizon. Data breach investigations report; 2019.
16. IBM Security. Cost of a data breach report; 2019.
17. Böhme R. A comparison of market approaches to software vulnerability disclosure. In: Emerging trends in ICT security; 2006. p. 298–311.
18. Dempsey K *et al*. Information security continuous monitoring (ISCM) for federal information systems. NIST SP 800-137; 2011.
19. Stouffer K Lightman S Pillitteri V Abrams M Hahn A. Guide to industrial control systems (ICS) security. NIST SP 800-82 Rev. 2; 2015.
20. Allodi L Massacci F. Comparing vulnerability severity and exploits using case-control studies. ACM Trans Inf Syst Secur. 2014;17(1).
21. Executive Order No. 13873. Securing the information and communications technology and services supply chain; 2019.
22. Department of Defense. Defense federal acquisition regulation supplement clause 252.204-7012; 2020.
23. Federal Information Security Modernization Act of 2014. Pub L No. 113-283; 2014.
24. Office of Management and Budget. Managing information as a strategic resource. OMB Circular A-130; 2016.
25. Biggio B Roli F. Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognit. 2018;84:317–331.
26. Papernot N McDaniel P Sinha A Wellman MP. SoK: Security and privacy in machine learning. In: Proc IEEE EuroS&P; 2018. p. 399–414.
27. Yang Q Zhang Y Dai W Pan SJ. Transfer learning. Cambridge (UK): Cambridge University Press; 2020.
28. Rose S Borchert O Mitchell S Connelly S. Zero trust architecture. NIST SP 800-207; 2020.
29. National Institute of Standards and Technology. Protecting controlled unclassified information in nonfederal systems. NIST SP 800-171 Rev. 2; 2020.
30. Johnson C *et al*. Guide to cyber threat information sharing. NIST SP 800-150; 2016.
31. Nieles M Dempsey K Pillitteri VY. An introduction to information security. NIST SP 800-12 Rev. 1; 2017.
32. Bello AD Elebe O Hammed NI Omoegun GO Abutu DE. An e-learning framework for improving digital literacy and responsible technology use in primary and secondary schools. IRE J. 2020;4(3).
33. Elebe O. Conceptual model for insider threat classification and risk modeling in complex digital systems; 2018.
34. Elebe O. Risk-based cybersecurity assurance and data availability limitations advances and future research opportunities; 2019.
35. Elebe O. Conceptual model for privacy-centric security engineering in digital and cloud computing systems; 2020.
36. International Organization for Standardization. Information security management systems—requirements. ISO/IEC 27001:2013; 2013.
37. International Organization for Standardization. Risk management—guidelines. ISO 31000:2018; 2018.
38. ISACA. COBIT 5: A business framework for the governance and management of enterprise IT; 2012.
39. Luttgens JT Pepe M Mandia K. Incident response and computer forensics. 3rd ed. New York: McGraw-Hill; 2014.
40. Cherepanov A Lipovsky R. Industroyer: Biggest threat to industrial control systems since Stuxnet. ESET Research; 2017.
41. Dragos Inc. TRISIS malware: Analysis of safety system targeted attack; 2017.
42. Williams T. The Purdue enterprise reference architecture. Instrum Control Syst. 1994;67(2):68–78.
43. Organisation for Economic Co-operation and Development. OECD principles on artificial intelligence; 2019.
44. McKinsey Global Institute. The next normal in construction; 2020.
45. Schneier B. Secrets and lies: Digital security in a networked world. Indianapolis (IN): Wiley; 2004.
46. Pfleeger C Pfleeger SL. Security in computing. 5th ed. Upper Saddle River (NJ): Prentice Hall; 2015.
47. SANS Institute. Critical security controls for effective cyber defense; 2018.
48. Ponemon Institute. State of cybersecurity in small and medium-sized businesses; 2019.
49. Whitman M Mattord H. Principles of information security. 5th ed. Stamford (CT): Cengage; 2017.
50. Stallings W. Cryptography and network security: Principles and practice. 7th ed. Hoboken (NJ): Pearson;

2017.
51. ENISA. Threat landscape report; 2019.
52. Anderson R. Security engineering: A guide to building dependable distributed systems. 3rd ed. Hoboken (NJ): Wiley; 2020.
53. Akomolafe O Agu MU. A conceptual model for enhancing internal audit quality through technology-enabled risk assessment frameworks. IRE J. 2018;1(9).
54. Akomolafe O Agu MU. A conceptual framework for developing risk-based internal control models in the insurance and banking sectors. IRE J. 2019;2(8).
55. Akomolafe O Agu MU. Advances in financial resilience through integrated governance and compliance strategies. IRE J. 2019;2(10).
56. Akomolafe O Agu MU. A review of data-driven risk evaluation models for emerging market financial institutions. IRE J. 2019;3(6).
57. Akomolafe O Olaogun BO Adesuyi MO Ndukwe VU Sakyi JK. Collaborative governance framework for secure cross-border payment data sharing. Int J Adv Multidiscip Res Stud. 2025;5(6):849–865.
58. Adesuyi MO Akomolafe O Olaogun BO Ndukwe VU Sakyi JK. AI-enabled fraud detection ecosystem model for securing international payment channels. Int J Adv Multidiscip Res Stud. 2025;5(6):866–882.
59. Akomolafe O Agu MU Bello A. A conceptual model for advancing risk governance through data-driven compliance analytics in financial institutions. J Account Financ Manage. 2025;11(11):211–228.
60. Agu MU Akomolafe O Bello A. Advances in predictive financial risk assessment using Python-based forecasting systems. Int J Comput Sci Math Theory. 2025;11(11):131–148.