International Journal of Cybersecurity Engineering and Innovation

ARTICLE INFO

Article History: Received: 20-04-2026, Revised: 20-06-2026, Accepted: 11-11-2026
Corresponding author Email: hsopheaktra.phdscholar@lincoln.edu.my

This is an open access article under the **CC BY 4.0 license** (http://creativecommons.org/licenses/by/4.0/).

Published by ITAP Publisher.



Vol. 2027 No.1

A Comprehensive Cyber Risk Measurement Framework Using Key Risk Indicators (KRIs) for Enterprise Risk Governance

Sopheaktra Huy[1*], Mony Ho[2], Sokroeurn Ang[3], Midhunchakkaravarthy Janarthanan[4]

[1]School of AI Computing and Multimedia, Lincoln University College, Selangor, Malaysia, hsopheaktra.phdscholar@lincoln.edu.my, https://orcid.org/0009-0006-7383-1667

[2] School of AI Computing and Multimedia, Lincoln University College, Selangor, Malaysia, angsokroeurn.phdscholar@lincoln.edu.my, https://orcid.org/0009-0000-9746-5469

[3] School of AI Computing and Multimedia, Lincoln University College, Selangor, Malaysia, mho.phdscholar@lincoln.edu.my, https://orcid.org/0009-0004-3389-1951

[4] School of AI Computing and Multimedia, Lincoln University College, Selangor, Malaysia, vivekanandam@lincoln.edu.my

Abstract

Organizations across all industries continue to face challenges in quantifying and monitoring cyber risk in a consistent, actionable, and predictive manner. Although cybersecurity frameworks such as NIST CSF, ISO/IEC 27001, and COBIT provide guidance for establishing controls, they offer limited support for operationalizing cyber risk measurement. Traditional qualitative assessments often rely on subjective scoring and static evaluations that fail to reflect the dynamic nature of cyber threats. This research addresses these limitations by proposing a comprehensive cyber risk measurement framework grounded in Key Risk Indicators (KRIs). The framework introduces a multi-domain taxonomy encompassing technology, human behavior, governance processes, and external threat conditions, supported by a quantitative scoring and threshold model that enables objective and comparable measurement. It further provides an integration approach for embedding KRIs into governance reporting and a five-level maturity model that guides organizations in developing their KRI capabilities. Drawing on design science research principles, the framework synthesizes cybersecurity standards, academic literature, and industry practices to deliver a practical and sector-agnostic method for transforming fragmented security metrics into data-driven cyber risk intelligence. The proposed framework enhances predictive risk management, strengthens decision-making, and supports continuous improvement in organizational cyber resilience. Practically, the framework supports risk managers, auditors, and boards in transitioning from fragmented security metrics to governance-ready cyber risk intelligence that enables timely prioritization and accountable decision-making.

Keywords: Quantum computing, Critical infrastructure protection, Post-quantum cryptography, Artificial intelligence, Cybersecurity risk mitigation.

1. Introduction

The accelerating digitalization of modern organizations has amplified their exposure to cyber threats, leading to an environment where cyber risk has become a critical component of enterprise risk management. Despite widespread adoption of cybersecurity frameworks such as NIST CSF, ISO/IEC 27001, and COBIT, many organizations continue to face difficulties in quantifying cyber risk in a consistent, objective, and actionable manner. Traditional cyber risk assessments often rely on qualitative judgments, subjective scoring, and periodic evaluations that fail to reflect the dynamic nature of cyber threats [1]. As a result, decision-makers lack reliable indicators for predicting incidents, prioritizing controls, or evaluating the effectiveness of security investments.

Key Risk Indicators (KRIs) offer a potential mechanism for bridging this measurement gap. In enterprise risk management, KRIs serve as early warning signals that quantify the likelihood or impact of adverse events [2]. However, while KRIs are well established in operational and financial risk domains, their application to cyber risk remains fragmented, inconsistent, and organization-specific. Existing cyber KRIs are typically developed ad hoc and lack standardization across industries [3]. Moreover, most published frameworks do not provide a structured taxonomy, classification methodology, or scoring model that organizations can use to operationalize KRIs as part of their cyber risk governance [4].

This research addresses these limitations by proposing a comprehensive cyber risk measurement framework grounded in KRIs. The framework introduces (1) a multi-dimensional KRI taxonomy, (2) a structured approach to scoring and threshold-setting, (3) an integrated reporting model for cyber risk dashboards, and (4) a maturity model that guides organizations in embedding KRIs into strategic and operational decision-making. The proposed model is designed to be sector-agnostic and applicable across diverse industries including finance, healthcare, manufacturing, telecommunications, and the public sector.

The primary contribution of this study is the development of a practical, measurable, and consistent approach to cyber risk quantification that supports continuous monitoring and enhances situational awareness. By synthesizing global standards, academic literature, and industry best practices, this research provides a unified method for transforming qualitative cybersecurity assessments into data-driven risk intelligence [5]. The framework aims to empower organizations not only to measure cyber risk but also to anticipate emerging threats, allocate resources more effectively, and strengthen overall cyber resilience. Although empirical evaluation (e.g., expert validation or case studies) is positioned as future work, existing approaches remain fragmented across technical, operational, and governance domains, offering limited guidance on how cyber KRIs should be structured, scored, and operationalized within enterprise risk management.

This study addresses this gap by proposing a unified cyber risk measurement framework that integrates a multi-domain KRI taxonomy, quantitative scoring and threshold models, governance integration mechanisms, and a maturity roadmap for progressive adoption.
Accordingly, this study addresses the following objectives:
1. To develop a structured, multi-domain taxonomy for cyber KRIs;
2. To propose a quantitative scoring and threshold model for consistent cyber risk measurement;
3. To integrate cyber KRIs into enterprise risk governance and reporting; and
4. To define a maturity model guiding progressive KRI adoption.

Unlike existing studies that focus on isolated technical metrics or compliance-driven indicators, this research delivers an integrated, governance-oriented KRI framework that explicitly connects cyber risk measurement to enterprise risk decision-making.

2. Literature Review

2.1 Cyber Risk and Measurement Challenges

Traditional cybersecurity risk assessments rely heavily on qualitative approaches such as heat maps, expert judgment, and maturity scoring. These methods are widely criticized for subjectivity and inconsistency, especially across different evaluators and organizations [6]. Furthermore, qualitative assessments fail to reflect the dynamic and rapidly changing nature of cyber threats, making them insufficient for real-time risk monitoring in modern environments [7].

Quantifying cyber risk remains a challenge due to the complexity of attack vectors, interdependencies in digital ecosystems, and the scarcity of reliable incident and loss data [8]. Advanced quantitative models such as FAIR attempt to address this challenge, but their adoption is limited by complexity and data requirements [9]. Consequently, organizations increasingly seek operationally practical measurement mechanisms, leading to rising interest in KRIs as predictive indicators [40]. These challenges are well documented in cyber risk and cyber insurance literature, which highlights data scarcity, uncertainty, and measurement inconsistency as persistent obstacles to effective cyber risk quantification [27], [28], [29].

2.2 Key Risk Indicators in Enterprise Risk Management

KRIs were pioneered in enterprise risk management domains such as operational and financial risk. Their purpose is to provide measurable indicators that predict the likelihood or severity of undesirable events [10]. In these domains, KRIs are well-established tools used to monitor compliance breaches, process failures, fraud events, and credit exposures. However, cyber KRIs remain significantly underdeveloped. Research indicates that organizations often develop cyber KRIs in an informal, unstructured manner, which leads to inconsistent measurement practices [11]. Many organizations rely primarily on technical metrics such as vulnerability counts, patching delays, or intrusion attempts. These indicators, while useful, fail to capture broader human, governance, and environmental dimensions of cyber risk [12].

Several studies highlight the potential of KRIs to act as early warning signals when designed correctly [13]. Yet the literature reveals a clear gap: there is no widely accepted taxonomy, methodology, or cross-industry framework for developing and operationalizing cyber KRIs. Prior studies emphasize that effective KRIs must be predictive, decision-oriented, and aligned with enterprise risk management objectives rather than isolated technical metrics [30], [32].

2.3 Cybersecurity Standards and Their Limitations in Risk Measurement

NIST Cybersecurity Framework (CSF):
Provides functions and categories but does not prescribe KRIs or scoring models [1].

ISO/IEC 27001 and 27004:
ISO 27001 defines management controls; ISO 27004 introduces metrics but does not specify cyber KRIs [15], [16].

COBIT 2019:
Offers governance and performance metrics, but these are not tailored to cyber risk events nor structured as KRIs [4].

CIS Controls:
Focus on technical safeguards but lack risk-based indicators [14].

Basel Frameworks:
Define operational KRIs but not cyber-specific indicators [10].
Across all frameworks, a consistent limitation emerges: no existing standard provides a complete, actionable methodology for designing and measuring cyber KRIs.

Industry and professional bodies have also acknowledged the lack of standardized cyber KRIs and the need for more structured measurement approaches beyond control compliance [31].

2.4 Existing Cyber KRI Research and Identified Gaps

Academic and industry reports increasingly reference cyber KRIs, but existing studies tend to be narrow in focus, emphasizing single-domain metrics such as vulnerabilities, phishing rates, or patch management indicators [19]. Most do not propose a structured taxonomy or unified methodology. Key gaps identified include:

1. Lack of a cross-industry KRI taxonomy covering technical, human, governance, and external threat dimensions
2. Absence of standardized scoring or threshold-setting methods
3. Limited integration of KRIs into enterprise risk governance
4. No maturity model describing organizational evolution in cyber KRI adoption
5. Insufficient research linking KRIs to predictive cyber risk management [20]

These gaps justify the need for a new, structured framework.

Recent research has demonstrated the effectiveness of machine learning–based security frameworks in detecting anomalies5 and improving cyber threat responsiveness. However, such approaches primarily focus on technical detection mechanisms and lack integration with enterprise risk governance, standardized scoring models, or maturity-based adoption roadmaps. This reinforces the need for a governance-oriented KRI framework that bridges technical analytics with enterprise risk decision-making [40].

2.5 Summary of Literature Gaps

The literature consistently indicates the need for:

- A comprehensive KRI framework
- A structured classification taxonomy
- Quantitative scoring methodologies
- Integration with risk governance
- A maturity model supporting continuous improvement

Collectively, these gaps highlight the absence of an integrated, operational, and governance-oriented cyber risk measurement approach. Existing studies either focus on isolated technical metrics or high-level qualitative frameworks, reinforcing the need for a unified KRI-based framework that supports measurement, governance, and maturity progression.

Table 1: Comparison of Existing Cyber Risk Measurement Approaches

Framework / Model	Cyber-Specific KRIs	Quantitative Scoring	Governance Integration	Predictive Focus	Maturity Model
NIST CSF	X	X	Partial	X	X
ISO/IEC 27001	X	Limited	Partial	X	X
COBIT 2019	X	Limited	✓	X	X
FAIR	Limited	✓	X	Partial	X
Basel KRIs	X	✓	✓	X	X
Proposed Framework	✓	✓	✓	✓	✓

Table 2: Identified Gaps in Existing Cyber KRI Research

Gap Area	Description
Taxonomy	Lack of unified cyber KRI structure
Measurement	Absence of standardized scoring and thresholds
Governance	Weak integration with ERM and board reporting
Predictive Value	Overreliance on lagging indicators
Maturity	No roadmap for KRI adoption evolution

These gaps collectively motivate the need for a unified, operational, and governance-integrated cyber risk measurement framework, which this study addresses through a design science approach. Recent international policy and governance reports further reinforce the need for integrated, governance-oriented cyber risk measurement models [33], [34], [35].

3. Methodology

3.1 Research Approach: Design Science Research (DSR)

This study adopts a Design Science Research (DSR) methodology to develop a comprehensive cyber risk measurement framework using KRIs. DSR is widely used in information systems research for creating and evaluating innovative artifacts such as models, frameworks, and taxonomies [21]. Unlike explanatory research, which focuses on describing phenomena, DSR emphasizes problem-solving, artifact construction, and practical relevance.

The choice of DSR is justified because existing cybersecurity standards and academic literature do not offer a unified method for designing and operationalizing cyber KRIs. DSR provides a structured process for synthesizing knowledge from standards, best practices, and prior research to create an artifact that fills a clearly identified gap [22].

Following guidelines by Hevner et al. [21], the research process incorporates the core DSR activities:

1. Problem identification and motivation
2. Definition of objectives for the solution
3. Design and development of the framework
4. Demonstration of applicability through examples
5. Evaluation through theoretical alignment and expert validation (in future research)
6. Communication of findings

This paper focuses on steps 1-4 and 6, providing a validated conceptual foundation for operational cyber KRI frameworks. The design science approach is particularly suitable for cybersecurity risk management research, where the objective is not only to explain phenomena but to develop actionable artifacts that can be adopted by organizations and evaluated through future empirical studies. The use of maturity models and staged capability development is consistent with established design and process improvement research in information systems and risk management [36].

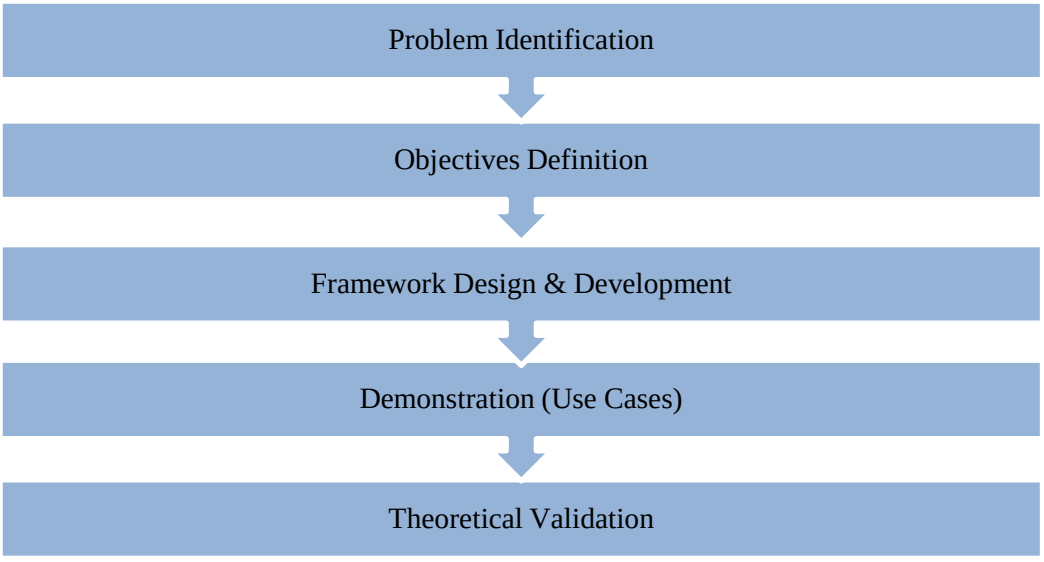

Figure 1. Design Science Research Process Applied in This Study

Consistent with early-stage design science research, this study focuses on conceptual validation through alignment with established standards, academic literature, and industry practices. Formal empirical evaluation through case studies or expert assessment is intentionally positioned as future work.

3.2 Framework Development Steps

The proposed framework was developed through a structured, iterative process consisting of four major phases.

Phase 1: Literature and Standards Review
The study reviewed academic literature, industry reports, and cybersecurity standards to identify recurring themes, limitations, and gaps in existing cyber KRI approaches. Frameworks analyzed included NIST CSF, ISO/IEC 27001 and 27004, COBIT 2019, CIS Controls, PCI DSS, Basel II/III, and COSO ERM.

Phase 2: KRI Domain Identification
Based on synthesis of prior research, four core domains of cyber risk were identified:

1. Technology and infrastructure risk
2. Human and behavioral risk

3. Process and governance risk
4. External threat and environmental risk

These domains form the foundation for a structured KRI taxonomy.

Phase 3: Development of Measurement Models

A quantitative scoring model was developed to enable objective evaluation of KRIs. This included defining:

- Indicator characteristics
- Numeric scales
- Threshold levels
- RAG (Red, Amber, Green) classifications
- Weighting mechanisms

This step ensures KRIs are measurable, comparable, and actionable.

Phase 4: Construction of the Cyber KRI Maturity Model

A five-level maturity framework was developed to guide organizations in their progressive adoption of KRIs. The model draws inspiration from capability maturity principles used in prior governance and risk research [23].

3.3 KRI Selection Criteria

To ensure relevance and usability, each KRI in the proposed framework is evaluated against a set of criteria synthesized from risk management literature and industry standards [24], [25]. Indicators must be:

1. Measurable: Quantifiable using consistent metrics and available data sources
2. Predictive: Able to indicate the likelihood of a future cyber event, not only record past incidents
3. Relevant: Directly connected to a meaningful area of cyber risk exposure
4. Actionable: Support decision-making, prioritization, or resource allocation
5. Comparable: Allow benchmarking across time periods or organizational units
6. Cost-effective: Not overly burdensome to collect or maintain

These criteria ensure that KRIs are practical and aligned with risk governance requirements.

3.4 Sources of Evidence Used in Framework Development

The framework is grounded in multiple evidence sources to ensure academic rigor and practical relevance:

(a) **Academic Literature**

Peer-reviewed studies related to cyber risk quantification, KRIs, security metrics, and enterprise risk management provided theoretical foundations [6], [8], [10].

(b) **Cybersecurity Standards and Guidelines**

Key standards such as NIST CSF, ISO 27001/27004, COBIT 2019, CIS Controls, and ENISA methodologies were analyzed for mapping controls to measurable indicators.

(c) **Industry Reports**

Publications from ENISA, PwC, Deloitte, Gartner, ISACA, and financial regulators were reviewed to identify emerging best practices and commonly used cyber KRIs [11], [12], [14].

(d) **Practitioner Use Cases**

Sample KRIs from various industries (finance, healthcare, manufacturing, government) were examined to ensure cross-industry applicability.

This triangulation of evidence supports the robustness and generalizability of the resulting framework.

3.5 Methodological Contribution

The methodology contributes to cyber risk management research by:

- Creating a unified, measurable KRI framework
- Introducing a structured KRI taxonomy
- Providing a quantitative scoring model

- Establishing a maturity model for KRI adoption
- Bridging a gap between cybersecurity standards and risk measurement literature

This positions the research as a novel and practical contribution to the field of cybersecurity risk management.

4. Proposed Cyber Risk Measurement Framework

Figure 2 illustrates the overall structure of the proposed cyber risk measurement framework, highlighting the interaction between KRI domains, scoring mechanisms, governance integration, and maturity progression. This section introduces a comprehensive measurement framework designed to standardize the selection, categorization, scoring, and governance integration of cyber KRIs. The framework consists of four components:

1. A structured KRI taxonomy
2. A quantitative scoring and threshold model
3. An integration model for reporting and governance, and
4. A five-level maturity model for KRI adoption

The framework is designed to be industry-agnostic, allowing organizations from diverse sectors to adapt it according to their operational context and regulatory obligations.

4.1 Key Risk Indicator (KRI) Taxonomy

Existing literature lacks a unified structure for organizing cyber KRIs across functional domains. To address this gap, a four-domain taxonomy is proposed, synthesizing elements from cybersecurity standards, enterprise risk management frameworks, and empirical industry practices [14], [18], [19], [4], [15].

Domain 1: Technology and Infrastructure Risk

KRIs reflecting the security posture of IT systems, networks, and platforms.
Examples include:

- Percentage of critical vulnerabilities unpatched beyond SLA
- Number of high-risk configuration deviations
- Frequency of system outages affecting critical services
- Endpoint protection coverage rate
- Mean time to detect (MTTD) and mean time to respond (MTTR)

These indicators capture control effectiveness, technology resilience, and exposure to technical threats.

Domain 2: Human and Behavioral Risk

KRIs measuring human factors, awareness, and insider threat exposure.
Examples include:

- Phishing simulation failure rate
- Frequency of privileged access misuse incidents
- Number of security awareness training non-completions
- Rate of policy violations
- Percentage of unresolved insider threat alerts

These indicators address the human layer, which research identifies as a leading cause of cyber incidents [12], [20].

Domain 3: Process and Governance Risk

KRIs evaluating process maturity, policy compliance, and governance effectiveness.
Examples include:

- Percentage of overdue risk assessments
- Number of audit findings related to cybersecurity controls
- SLA breaches in patch or change control processes
- Third-party compliance gaps
- Number of exceptions granted to security policies

This domain aligns with governance frameworks such as COBIT and ISO 27001’s management controls

[15], [16].

Domain 4: External Threat and Environmental Risk
KRIs that reflect threat landscape fluctuations and external risk exposures.
Examples include:

- Volume of detected threat intelligence alerts
- Number of attempted cyberattacks targeting the organization
- Sector-wide vulnerability disclosures (e.g., zero-days)
- Level of geopolitical cyber activity
- Supply chain security posture scores

This domain supports monitoring of external pressures, enabling proactive risk adjustments [17].

Table 3: Cyber KRI Taxonomy by Risk Domain

Domain	Risk Focus	Example KRIs
Technology	Infrastructure resilience	MTTD, MTTR, unpatched vulnerabilities
Human	Insider & awareness risk	Phishing failure rate, policy violations
Governance	Process maturity	Audit findings, overdue risk assessments
External	Threat landscape	Zero-days, threat intelligence volume

4.2 KRI Scoring and Threshold Model

To standardize measurement, this framework introduces a quantitative scoring model with RAG (Red-Amber-Green) thresholds. The scoring approach follows three principles:

1. Objectivity: Results based on numeric values, not subjective judgment
2. Comparability: Metrics remain consistent across units and time periods
3. Actionability: Each threshold corresponds to required management actions

4.2.1 Indicator Scoring Scale

Each KRI is scored on a 1-5 scale:

- 1 = Very Low Risk
- 2 = Low Risk
- 3 = Moderate Risk
- 4 = High Risk
- 5 = Critical Risk

This scale aligns with common enterprise risk scoring models used in operational and technology risk management [24].

Table 4: KRI Scoring Scale and Risk Interpretation

Score	Risk Level	Interpretation	Required Action
1-2	Low	Within tolerance	Maintain controls
3	Medium	Deviation emerging	Monitor & review
4-5	High	Exceeds appetite	Escalate & remediate

4.2.2 Threshold Setting

Thresholds must be tailored to the organization but follow general patterns.

Table 5: KRI Scoring Thresholds

Score	Threshold Description	Example Interpretation
1-2 (Green)	Within risk tolerance	Vulnerabilities patched within SLA; low phishing failure rate
3 (Amber)	Deviation requires monitoring	Moderate number of overdue risk assessments
4-5 (Red)	Exceeds risk appetite	High number of critical unpatched vulnerabilities; increasing insider threat alerts

4.2.3 Weighting Model

Not all Key Risk Indicators (KRIs) contribute equally to an organization's overall cyber risk exposure. To reflect differing levels of criticality, this framework applies a weighting factor w_i to each KRI. The weighted aggregation enables more accurate representation of organizational risk priorities.

The overall cyber risk score is calculated as:

$$\text{Risk Score} = i=1 \sum n(KRIi \times wi) \quad (1)$$

Where:

- KRI_i represents the normalized score of the *i*-th Key Risk Indicator (typically on a 1-5 scale),
- w_i represents the relative weight assigned to that KRI, reflecting its importance to the organization, and
- n represents the total number of KRIs included in the aggregation.

1. **A. Weight Assignment Criteria**

Weights are assigned based on organizational context and risk priorities, commonly considering the following factors:

- **Business criticality**: Degree to which the KRI affects critical business services or revenue-generating systems
- **Regulatory significance**: Alignment with regulatory requirements, supervisory expectations, or compliance obligations
- **Impact potential**: Potential financial, operational, reputational, or safety impact if the risk materializes

Weights are typically normalized so that their sum equals 1.0 (or 100%), ensuring proportional contribution across indicators.

2. **B. Practical Example**

Assume an organization monitors three KRIs:

Table 6. Weighted KRI Scoring Example

KRI	Description	Score (1–5)	Weight
KRI_1	Critical vulnerability backlog	4	0.4

KRI_2	Phishing simulation failure rate	3	0.35
KRI_3	Overdue risk assessments	2	0.25

The aggregated cyber risk score is calculated as:

$$(4\times0.40)+(3\times0.35)+(2\times0.25)=1.60+1.05+0.50=3.15$$

This aggregated score provides management with a single, interpretable risk value that reflects both risk severity and organizational priorities.

3. **C. Benefits of Weighted Scoring**

The weighting model offers several advantages:

- Enables **risk-based prioritization** aligned with business objectives
- Prevents low-impact indicators from disproportionately influencing overall risk
- Supports **board-level reporting** through simplified, aggregated metrics
- Enhances comparability across time periods and organizational units

By incorporating weighted KRIs, organizations can move from fragmented technical metrics to **governance-ready cyber risk intelligence,** supporting informed decision-making and targeted risk mitigation.

4.3 Integration of KRIs into Cyber Governance

Effective use of KRIs requires integration into organizational governance structures. The proposed integration model aligns with enterprise risk management practices and cybersecurity oversight processes [10], [16], [25].



Figure 2. Integration of KRIs into Cyber Risk Governance

4.3.1 Cyber Risk Dashboard

KRIs are consolidated into a visual dashboard showing:

- Individual KRI scores

- RAG status
- Trends over time
- Aggregated risk scores by domain
- Heat maps or radar charts for executive reporting

Dashboards support communication with CISOs, CROs, and boards.

4.3.2 Governance Reporting

KRIs must be embedded into:

- Monthly cyber risk reports
- Quarterly risk committee packs
- Board-level cybersecurity updates
- Internal audit and compliance reviews

This ensures metrics support strategic decision-making and regulatory expectations.

4.3.3 Decision-Making Workflow

The framework links KRI thresholds to specific actions:

- **Green:** Maintain controls
- **Amber:** Initiate monitoring or process review
- **Red:** Escalate to senior management, launch remediation, allocate resources

A defined workflow ensures KRIs drive timely and accountable actions.

4.4 Cyber KRI Maturity Model

Figure 3 presents the five-level Cyber KRI Maturity Model, outlining the progressive evolution of organizational KRI capabilities from ad hoc practices to optimized, predictive risk management.

A five-level maturity model guides organizations in progressively improving their KRI capabilities, inspired by capability maturity models in cybersecurity and governance literature [23].

Level 1: Ad Hoc

- No formal KRI program
- Indicators used inconsistently
- Data quality issues prevalent

Level 2: Developing

- Initial KRIs defined
- Basic reporting begins
- Limited automation

Level 3: Defined

- KRI taxonomy established
- Standardized scoring and thresholds in place
- Regular reporting implemented

Level 4: Quantitatively Managed

- Comprehensive dashboards
- Automated data collection
- KRIs linked to predictive modelling

Level 5: Optimized

- KRIs continuously improved
- Integrated with enterprise risk systems
- Predictive analytics and AI used for forecasting

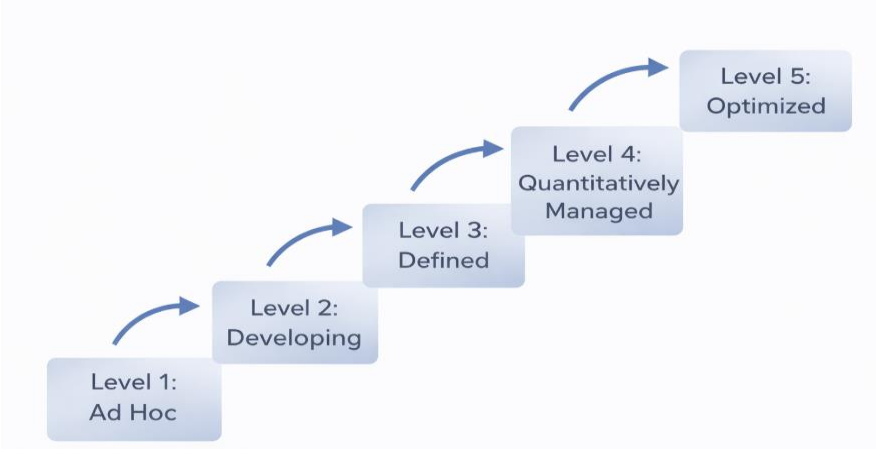

Figure 3. Proposed levels

This model provides organizations with a roadmap for maturing their cyber risk measurement capability. The proposed maturity structure is further supported by prior cybersecurity maturity model research and systematic reviews of maturity-based risk frameworks [37].

Table 7. Cyber KRI Maturity Model

Level	Name	Characteristics
1	Ad Hoc	No formal KRIs
2	Developing	Initial KRIs defined
3	Defined	Standardized taxonomy & scoring
4	Managed	Dashboards & automation
5	Optimized	Predictive analytics & AI

5. Discussion

The proposed cyber risk measurement framework addresses significant limitations identified in existing literature and industry practices. By introducing a structured taxonomy, a quantitative scoring model, and an integration and maturity approach, the framework provides organizations with a holistic method to measure and monitor cyber risk in a consistent, actionable, and scalable manner. This section discusses the contributions, applicability, and implications of the framework, as well as its alignment with standards and comparison to existing models.

5.1 Theoretical Contributions

This research contributes to cybersecurity and risk management theory in several ways. First, it establishes a multi-domain KRI taxonomy that reflects the multidimensional nature of cyber risk, incorporating technological, human, governance, and environmental factors. Existing literature often treats these domains separately, focusing predominantly on technical metrics [11], [19]. The taxonomy introduced in this study unifies them into a coherent structure, extending the conceptual understanding of cyber risk measurement.

Second, the research provides a quantitative scoring approach aligned with enterprise risk management principles. While many organizations rely on qualitative assessments, few academic works propose numeric KRI-based scoring models that can support objective decision-making [6], [8]. This study fills that gap by defining thresholds, scales, and weighting mechanisms that enable measurable and comparable risk insights.

5.2 Practical and Managerial Implications

The proposed framework delivers several practical benefits for cybersecurity leaders, risk managers, and decision-makers. For risk oversight bodies such as risk committees, internal audit, and regulators, the proposed framework provides a standardized mechanism for evaluating cyber risk exposure beyond compliance-based reporting. This supports stronger assurance, benchmarking, and supervisory review processes, particularly in highly regulated sectors such as banking and critical infrastructure.

Table 8. Stakeholder-Specific Benefits of the Framework

Stakeholder	Benefit
CISO	Early warning & prioritization
CRO	Quantified risk aggregation
Board	Comparable cyber risk reporting
Internal Audit	Risk-based audit planning
Regulators	Improved assurance & oversight

5.2.1 Improved Predictive Risk Management

KRIs function as early warning indicators that enable organizations to anticipate cyber incidents rather than merely documenting past events. By incorporating predictive indicators across technology, human, governance, and external threat domains, organizations can identify emerging risks before they escalate [12]. Prior research highlights that combining internal security indicators with external intelligence significantly enhances predictive cyber risk monitoring and situational awareness [38]. Recent machine learning–based security frameworks further demonstrate how predictive analytics can strengthen early threat detection and proactive cyber risk management, reinforcing the value of forward-looking KRIs [40].

5.2.2 Standardized and Repeatable Measurement

The scoring model enables consistent measurement across business units, departments, and time periods. This reduces subjectivity inherent in qualitative risk methods and supports a data-driven risk culture [7].

5.2.3 Better Cyber Governance and Reporting

Integrating KRIs into dashboards, risk committees, and executive reporting strengthens governance structures. Boards increasingly demand quantifiable metrics to evaluate cybersecurity posture and allocate resources [16], and this framework provides the structure to support those expectations.

5.2.4 Resource Prioritization

By assigning weights and providing aggregated scores, the framework supports prioritized investment in control enhancements, staffing, training, and technology initiatives. High-risk areas identified through KRI scoring can be addressed proactively.

5.2.5 Applicability across Industry Sectors

The sector-agnostic taxonomy ensures relevance in:

- Finance
- Healthcare
- Manufacturing
- Telecommunications
- Energy and utilities
- Public administration

This broad applicability enhances the framework's utility for regulators and large enterprises operating across multiple jurisdictions.

From an assurance perspective, the framework also supports risk-based auditing and regulatory supervision by providing consistent, traceable, and quantitative indicators of cyber risk exposure. This enables internal auditors and regulators to move beyond control compliance toward continuous, risk-informed oversight.

5.3 Comparison with Existing Measurement Models

Several cyber risk measurement models exist, but none offer a comprehensive KRI-based approach.

Qualitative Frameworks

Most cybersecurity frameworks such as NIST CSF and ISO 27001—guide organizations in establishing controls but lack quantitative measurement methods [1], [15]. They do not provide standardized scoring approaches or KRI selection methodologies.

Technical Metrics Models

Industry approaches often focus on technical indicators such as vulnerability counts or patch compliance [19]. While useful, these indicators only capture a portion of the cyber risk landscape and overlook human and governance dimensions. Empirical studies on vulnerability disclosure and patching behavior further demonstrate why lagging technical metrics alone are insufficient for proactive cyber risk management [39].

FAIR and Quantitative Impact Models

Models such as FAIR emphasize financial quantification but require extensive data and advanced modelling that many organizations lack [9]. FAIR also focuses on impact estimation rather than operational KRIs.

Operational Risk KRI Models

Basel frameworks introduce KRIs in financial risk management but do not address cyber-specific risks or technical controls [18].

In contrast, the proposed framework:

- Integrates multiple risk domains
- Includes both leading and lagging indicators
- Provides a full scoring model and maturity approach
- Aligns with but extends existing standards
- Requires minimal specialized data or tooling

Thus, the framework fills a practical and conceptual gap by merging the strengths of multiple approaches into a unified measurement system.

5.4 Cross-Industry Adaptability

A key strength of the framework is its adaptability across industries. This is possible due to two characteristics:

1. Universal Cyber Risk Domains

Regardless of sector, organizations rely on technology, employ people, follow governance processes, and operate in an external threat landscape. Thus, the four KRI domains have broad relevance.

2. Flexible Scoring and Thresholds

Organizations can tailor thresholds, weights, and metrics based on:

- Regulatory requirements
- Organizational size and complexity
- Industry-specific risk appetite

This flexibility enables adoption in both highly regulated sectors (e.g., finance, healthcare) and less regulated environments (e.g., small enterprises, manufacturing).

5.5 Limitations of the Proposed Framework

While the framework offers significant contributions, several limitations must be acknowledged. Additionally, the proposed scoring and weighting mechanisms may require calibration to reflect organizational risk appetite and regulatory context, which may introduce variability across implementations.

Despite these limitations, the framework establishes a robust conceptual foundation that can be incrementally operationalized and empirically validated as organizational data maturity improves.

5.5.1 Data Quality and Availability

KRIs rely on accurate and timely data. Organizations lacking mature monitoring systems may struggle to collect high-quality data for certain indicators.

5.5.2 Need for Organizational Customization

Although the taxonomy is universal, the specific KRIs and thresholds must be customized. This introduces variation across industries and organizations.

5.5.3 Limited Empirical Validation

The framework is conceptual and informed by standards and industry practices. Future empirical validation—through case studies, expert evaluation, or surveys—is required to assess practical performance.

5.5.4 Dynamic Threat Landscape

External threat indicators may rapidly evolve, requiring organizations to periodically update KRIs to remain relevant [17]. Despite these limitations, the framework provides a structured foundation for future empirical research and practical implementation.

5.6 Implications for Risk Auditing and Assurance

The proposed KRI-based measurement approach strengthens assurance and audit functions by enabling risk-based prioritization and evidence-driven oversight. For internal audit planning, KRIs can be used to identify control areas with deteriorating trends (e.g., persistent patch SLA breaches, increasing phishing failures, or repeated policy exceptions), thereby improving audit scoping and resource allocation. In risk-based audit execution, domain-level KRI scores provide auditable evidence to support control testing strategies and to validate whether remediation actions produce measurable improvement over time.

At the board reporting level, standardized KRI dashboards improve transparency and comparability by translating technical security signals into risk-focused indicators aligned with risk appetite and escalation thresholds. For regulators and supervisory reviews, the framework provides a structured mechanism for demonstrating continuous monitoring, governance accountability, and a maturity-based improvement roadmap. Overall, the integration of KRIs into audit and assurance supports stronger cyber risk oversight beyond compliance-based reporting.

6. Conclusion and Future Work

Cyber risk has become a critical concern for modern organizations as digital ecosystems expand and the threat landscape grows increasingly complex. Despite the proliferation of cybersecurity frameworks such as NIST CSF, ISO/IEC 27001, and COBIT, a persistent gap remains in the ability of organizations to consistently quantify cyber risk and translate security performance into meaningful governance insights. Traditional qualitative assessments lack objectivity, predictability, and comparability, limiting their effectiveness for decision-making in dynamic environments [6], [7].

To address this challenge, this study proposed a comprehensive cyber risk measurement framework grounded in Key Risk Indicators (KRIs). The framework introduces four major contributions:

1. A multi-domain KRI taxonomy that captures technology, human, governance, and external threat dimensions;
2. A quantitative scoring and threshold model that standardizes measurement and supports risk prioritization;
3. An integration model for embedding KRIs into governance processes, dashboards, and reporting structures;
4. A five-level maturity model that guides organizations in progressively enhancing their cyber KRI capabilities.

The framework is intentionally designed to be sector-agnostic and adaptable across diverse industries, addressing limitations in existing research, which often focuses on isolated indicators, narrow metrics, or sector-specific use cases [11], [19]. By offering a structured, actionable, and scalable approach, this study equips organizations with a practical tool for enhancing situational awareness, strengthening predictive risk management, and improving communication between cybersecurity functions and executive stakeholders.

From a theoretical standpoint, the research contributes to the advancement of cyber risk measurement by bridging the gap between enterprise risk management concepts and cybersecurity operational realities. Practically, it provides organizations with a structured roadmap for transforming fragmented metrics into a unified, data-driven risk intelligence system.

However, several limitations must be acknowledged. The framework is conceptual and has not yet undergone empirical validation through real-world implementation or case studies. Data availability, organizational maturity, and contextual differences may affect the ease of adoption, and certain domains, especially external threat indicators-require regular updates to remain relevant in a rapidly evolving threat environment.

Future research should focus on expanding and validating the framework. Key areas include:

- Empirical evaluation through case studies in multiple industries;
- Development of automated KRI monitoring systems using SIEM, SOAR, and telemetry data;
- Integration of AI and machine learning to enhance predictive accuracy and automate scoring;
- Sector-specific adaptations, such as tailored KRI sets for banking, healthcare, manufacturing, or government;
- Longitudinal studies to assess how KRI maturity evolves over time.
- Integration of machine learning–based anomaly detection techniques with KRI scoring models to enhance predictive cyber risk intelligence, building on recent advances in ML-driven security frameworks [40].

Overall, this study contributes a practical and theoretically grounded foundation for advancing cyber risk measurement, bridging the long-standing gap between qualitative cybersecurity assessments and quantitative enterprise risk management practices. In practical terms, the framework provides organizations with a structured pathway to move from fragmented security metrics to governance-ready cyber risk intelligence that supports timely prioritization and accountable decision-making.

Declarations

Acknowledgements
NA

Funding
NA

Contributions
All authors; Conceptualization, All authors; Investigation; All authors; Writing (Original Draft), All authors; Writing (Review and Editing) Supervision, All authors; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Data Availability Statement
The authors thank their co-authors for guidance, peer reviewers for valuable feedback, and all participants for their contributions. They also acknowledge the support of the Lincoln University College Doctoral Program and appreciate the editorial team and anonymous reviewers of the Journal of Security Risk Management for their constructive input.

Use of Generative Artificial Intelligence
The authors declare that no generative artificial intelligence tools were used in the preparation of this manuscript.

Competing interests
All authors declare no competing interests.

References

[1] National Institute of Standards and Technology. (2023). *NIST cybersecurity framework (CSF) 2.0*. https://www.nist.gov/cyberframework
[2] Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management—Integrating with strategy and performance*.
[3] Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, *3*(3), 327-350.
[4] ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*.

[5] Bernardo, L., Malta, S., & Magalhães, J. (2025). An evaluation framework for cybersecurity maturity aligned with the NIST CSF. *Electronics*, *14*(7), 1364.
[6] Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. Wiley. https://doi.org/10.1002/9781119085294
[7] Gartner. (2023). *Top cybersecurity trends and challenges for 2023*. Gartner Research.
[8] Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001
[9] Ludvigson, S. C., & Ng, S. (2007). The empirical risk–return relation: A factor analysis approach. *Journal of financial economics*, *83*(1), 171-222.
[10] Basel Committee on Banking Supervision. (2011). *Principles for the sound management of operational risk*. Bank for International Settlements.
[11] PwC. (2022). *Global digital trust insights survey 2022*. PwC Global.
[12] Verizon. (2023). *Data breach investigations report 2023*. Verizon Enterprise.
[13] Böhme, M., & Kataria, G. (2020). *Models of cyber risk*. Workshop on the Economics of Information Security. https://doi.org/10.48550/arXiv.2005.08168
[14] Center for Internet Security. (2021). *CIS critical security controls v8*.
[15] International Organization for Standardization, & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022—Information security management systems—Requirements*. International Organization for Standardization.
[16] International Organization for Standardization, & International Electrotechnical Commission. (2016). *ISO/IEC 27004:2016—Information security management—Monitoring, measurement, analysis and evaluation*. International Organization for Standardization.
[17] Microsoft. (2023). *Microsoft digital defense report 2023*. Microsoft Security.
[18] Calvo, M., & Beltrán, M. (2024). Applying the Goal, Question, Metric method to derive tailored dynamic cyber risk metrics. *Information & Computer Security*, *32*(2), 133-158.
[19] Accenture. (2023). *State of cybersecurity resilience 2023*. Accenture Security.
[20] IBM Security, & Ponemon Institute. (2023). *Cost of a data breach report 2023*. IBM.
[21] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.25300/MISQ/2004/28.1.05
[22] Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302
[23] Software Engineering Institute. (2018). *Capability maturity model integration (CMMI) v2.0*. Carnegie Mellon University.
[24] Ionescu, Ș., Dumitrescu, G., Ioanăș, C., & Delcea, C. (2024). Mapping the landscape of key performance and key risk indicators in business: A comprehensive bibliometric analysis. *Risks*, *12*(8), 125.
[25] Cernisevs, O., Popova, Y., & Cernisevs, D. (2023, June). Risk-based approach for selecting company key performance indicator in an example of financial services. In *Informatics* (Vol. 10, No. 2, p. 54). MDPI.
[26] Cernisevs, O., Popova, Y., & Cernisevs, D. (2023). Business KPIs based on compliance risk estimation. *Journal of Tourism and Services*, *14*(27), 222-248.
[27] Biener, C., Eling, M., & Wirfs, J. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance—Issues and Practice*, *40*(1), 131–158. https://doi.org/10.1057/gpp.2014.19
[28] Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122
[29] Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35–61. https://doi.org/10.1016/j.cosrev.2017.01.001
[30] Crelinsten, R. D. (1989). Terrorism, counter-terrorism and democracy: The assessment of national security threats. *Terrorism and Political Violence*, *1*(2), 242-269.
[31] Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & Security*, *65*, 77-89.
[32] Aven, T. (2016). Risk assessment and risk management: Review of recent advances. *European Journal of Operational Research*, *253*(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023
[33] Organisation for Economic Co-operation and Development. (2020). *Digital security risk management for economic and social prosperity*. OECD Publishing. https://doi.org/10.1787/ecd2ec57-en
[34] Slapničar, S., Axelsen, M., & Eulerich, M. (2025). Cyber risk management: an illusion of a risk-based approach. *Journal of Management Control*, 1-36.

[35] Awan, M. S. K., Burnap, P., & Rana, O. (2016). Identifying cyber risk hotspots: A framework for measuring temporal variance in computer network risk. *computers & security*, *57*, 31-46.
[36] Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model for software. *IEEE Software*, *10*(4), 18–27. https://doi.org/10.1109/52.219617
[37] Le, N. T., & Hoang, D. B. (2016, December). Can maturity models support cyber security?. In *2016 IEEE 35th international performance computing and communications conference (IPCCC)* (pp. 1-7). IEEE.
[38] Kott, A., & Arnold, C. (Eds.). (2013). *Cyber situational awareness: Issues and research*. Springer. https://doi.org/10.1007/978-3-319-04117-4
[39] Sabottke, C., Suciu, O., & Dumitraş, T. (2015). Vulnerability disclosure and patching behavior. In *Proceedings of the 24th USENIX Security Symposium*.