ISSN 1648-0627 / eISSN 1822-4202

VILNIUS TECH
Vilnius Gediminas Technical University

BUSINESS: THEORY & PRACTICE

2026
Volume 27
Issue 2
Pages 282–297
https://doi.org/10.3846/btp.2026.25873

CYBER RESILIENCE EXPOSURE INDEX (CREI): TURNING THE ASSET-RISK MATRIX INTO A DECISION METRIC

Alona BAHMANOVA[1]✉, Viktorija STASYTYTĖ[2], Natalja LACE[3]

[1, 3]*Faculty of Engineering Economics and Management, Riga Technical University, Kalnciema iela 6, 1048 Riga, Latvia*
[2]*Institute of Dynamic Management, Vilnius Gediminas Technical University, Saulėtekio al. 11, 10223 Vilnius, Lithuania*

Article History:
- received 23 January 2026
- accepted 31 August 2026

Abstract. Small and medium-sized enterprises (SMEs) face disproportionate cyber risk exposure due to persistent financial, technical, and human resource constraints. Although cyber resilience has gained increasing attention, SMEs still lack practical quantitative instruments that enable structured measurement, comparison, and management of cyber risk exposure. This paper addresses this gap by proposing a risk-centric quantitative assessment model for SME cyber resilience. The study introduces the Cyber Resilience Exposure Index (CREI), a composite metric designed to quantify cyber risk exposure across critical organizational assets and major cyber risk categories. The index integrates four dimensions: likelihood-impact risk evaluation, weighted cyber risk categories, asset criticality, and cybersecurity control maturity as a mitigating factor. CREI is calculated across an asset-risk matrix and produces sector-comparable scores on a 0–100 scale, where lower exposure indicates higher resilience. Sensitivity analysis demonstrates the robustness of results under different weighting schemes, while a practical scoring guide and illustrative example support immediate SME adoption. The proposed metric operationalizes cyber resilience as a decision-oriented management tool, strengthening investment prioritization and enabling longitudinal benchmarking across sectors.

Keywords: cyber resilience, cyber risk exposure, small and medium-sized enterprises, risk quantification, composite index, asset-based risk assessment, decision-support model.

JEL Classification: G32, L26, O33.

✉Corresponding author. E-mail: *alona.bahmanova@edu.rtu.lv*

Abbreviations

AHP – Analytic Hierarchy Process;
AI – Artificial Intelligence;
CREI – Cyber Resilience Exposure Index;
ENISA – European Union Agency for Cybersecurity;
MCDM – Multi-Criteria Decision-Making;
NIST – National Institute of Standards and Technology;
SME – Small and Medium-sized Enterprise.

1. Introduction

Digital transformation has become a defining condition of contemporary business environments, reshaping how organizations create value, deliver services, and maintain competitiveness. Small and medium-sized enterprises (SMEs), in particular, increasingly depend on cloud services, interconnected digital infrastructures, data-driven processes, and AI-enhanced tools to sustain operational efficiency and respond to evolving market demands (Radanliev et al., 2020). However, this rapid technological integration exposes SMEs to a growing spectrum of cyber risks that disproportionately affect them compared to large enterprises. While larger organizations typically possess dedicated cybersecurity teams, established controls, and extensive financial buffers, SMEs operate under structural constraints that limit their ability to prevent, detect, and respond to cyber threats (Al-Hawamleh, 2024; Duraj et al., 2025; Rea-Guaman et al., 2018).

Recent research has demonstrated that SMEs face multidimensional exposure that spans external cyberattacks, insider misuse, data vulnerabilities, operational weaknesses, sophisticated AI-enabled threats, and reputational or financial consequences. Yet despite the extensive literature on cyber threats and resilience, a persistent gap remains in how SMEs can systematically measure their exposure

Copyright © 2026 The Author(s). Published by Vilnius Gediminas Technical University

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (*http://creativecommons.org/licenses/by/4.0/*), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

across diverse risk categories. Traditional risk assessment frameworks – such as the NIST Cybersecurity Framework or probabilistic risk models – require resources and expertise that SMEs often lack (Aven, 2016; NIST, 2018). As a result, SMEs rely primarily on qualitative assessments, subjective judgments, or fragmented checklists, which offer limited capacity for comparison, prioritization, or strategic planning (Aven & Zio, 2018; Taleb, 2012).

Authors' previous work addressed part of this challenge by proposing a structured asset-risk matrix that categorizes critical SME assets and maps them to six major cyber risk categories. While this matrix offered a conceptual foundation for understanding interdependencies and vulnerability patterns, its diagnostic power remained qualitative. Without quantification, the matrix cannot serve as a decision-making instrument capable of prioritizing investments, evaluating control effectiveness, benchmarking against peers, or supporting longitudinal resilience monitoring (Bahmanova & Lace, 2025a; 2025b).

To overcome this limitation, the present paper introduces the Cyber Resilience Exposure Index (CREI) – a novel quantitative metric that transforms the asset-risk matrix into a comprehensive, sector-comparable, and management-oriented decision tool. CREI operationalizes risk exposure by integrating four critical components:

- likelihood-impact scoring for each risk category (Stoneburner et al., 2002; Rasmussen, 1997),
- weighting of risk categories based on analytic methods such as the Analytic Hierarchy Process (AHP) and entropy analysis,
- criticality weights for organizational assets, and
- a control maturity factor representing the mitigating strength of implemented security controls.

The resulting index yields a normalized score from 0 to 100, where lower values correspond to lower exposure and, therefore, higher cyber resilience.

This approach contributes to academic and practical domains in three ways. First, it advances SME-focused cyber resilience research by introducing a measurable and replicable exposure metric that does not depend on historical incident data. Second, it bridges qualitative and quantitative assessment methods by embedding structured judgment into a mathematical scoring system. Third, it translates cybersecurity complexity into decision-ready information, helping SMEs identify high-leverage mitigation actions, allocate limited resources effectively, and align cyber resilience planning with strategic business priorities.

The objective of this study is to develop and demonstrate a quantitative, asset-based metric that enables SMEs to assess and interpret their cyber risk exposure in a structured and decision-oriented manner.

To achieve this objective, the study addresses the following research questions:

- RQ1: Which cyber risk categories and organizational assets are most critical for assessing cyber exposure in SMEs?
- RQ2: How can asset criticality, cyber risk likelihood, and cybersecurity control maturity be systematically integrated into a unified quantitative exposure metric?
- RQ3: How can the proposed Cyber Resilience Exposure Index support prioritization and decision-making in resource-constrained SMEs?

The remainder of this paper is structured as follows. Section 2 reviews the state of research on cyber resilience, asset-based risk assessment, and existing quantitative indices, highlighting limitations in SME applicability. Section 3 describes the methodological framework of CREI, including the weighting mechanisms, maturity model, and normalization procedures. Section 4 presents the mathematical formulation of the index and discusses underlying assumptions. Section 5 provides an illustrative example that demonstrates the practical application of CREI for an SME operating in a digitally intensive sector. Section 6 discusses implications for research and practice. Finally, the Conclusions summarize the study's contributions, outline its limitations, and indicate directions for future research.

2. Literature review

This literature review is grounded in the authors' previous peer-reviewed studies on cyber risk typologies and critical SME assets and was iteratively extended to support the development of a quantitative exposure index. As the research progressed, the literature base was supplemented with recent contributions addressing cyber resilience metrics, risk quantification, control maturity, and emerging cyber threats, ensuring conceptual continuity and methodological relevance.

The growing digitalization of SMEs has intensified scholarly attention toward cyber resilience as a critical condition for organizational sustainability. However, despite the expanding body of research, the literature remains fragmented across conceptual, asset-based, and quantitative strands. This section synthesizes existing studies relevant to the development of the CREI, focusing on four interrelated streams: cyber resilience in SMEs, asset-based cyber risk approaches, quantitative cyber risk indices, and the resulting research gap.

2.1. Cyber resilience in SMEs

Cyber resilience is commonly defined as an organization's ability to anticipate, withstand, recover from, and adapt to cyber incidents. Unlike traditional cybersecurity, which emphasizes prevention and protection, cyber resilience incorporates preparedness, response capacity, and adaptive learning (Yeboah-Ofori & Islam, 2019). For SMEs, this broader perspective is particularly relevant, as their limited resources, informal governance structures, and high dependence on digital technologies amplify the consequences of cyber disruptions (Saeed et al., 2023a; 2023b).

The literature consistently emphasizes that SMEs experience disproportionate cyber exposure compared to large enterprises. This imbalance arises not only from weaker technical defenses, but also from organizational characteristics such as limited cybersecurity expertise, lack of formalized processes, and constrained financial buffers. Studies highlight that SMEs often operate with fragmented security practices, relying on basic controls or reactive measures rather than systematic risk management.

Recent research further shows that digital transformation intensifies SME exposure by increasing reliance on cloud services, remote work infrastructures, data-driven processes, and AI-enabled tools. While these technologies enhance efficiency and competitiveness, they simultaneously expand the attack surface and introduce new categories of cyber risks. Importantly, the literature converges on the idea that SMEs require resilience-oriented approaches that move beyond compliance checklists or static maturity models.

Recent literature further emphasizes the growing role of AI-enabled cyber threats in reshaping the cyber risk landscape for SMEs. Artificial intelligence has become a dual-use technology: while it strengthens threat detection, monitoring, and automated incident response, it also enables adversaries to conduct more scalable, adaptive, and convincing attacks. Contemporary studies and cybersecurity reports highlight the increasing use of generative AI for phishing, vishing, synthetic identities, deepfake-enabled fraud, automated social engineering, malware adaptation, and vulnerability discovery.

These developments are particularly relevant for SMEs because AI-enabled attacks reduce the cost and effort required by attackers while increasing the difficulty of detection for organizations with limited cybersecurity expertise and resources. As a result, AI-driven threats intensify the need for practical, adaptive, and regularly updated cyber exposure assessment tools such as CREI. Recent research also highlights the growing importance of AI-supported cybersecurity mechanisms for both threat detection and cyber resilience enhancement. Artificial intelligence is increasingly used for advanced threat detection, cyber threat intelligence, adversarial machine learning, predictive analytics, explainable AI, automated risk assessment, and insider threat prevention (Dhanushkodi & Thejas, 2024; Ijiga et al., 2024; Singh & Dubey, 2024; Sarker et al., 2024; Muhammad et al., 2025; Sarfraz et al., 2025; Shafiq et al., 2026). At the same time, generative AI technologies enable increasingly sophisticated phishing campaigns, social engineering attacks, synthetic identities, and other forms of cyber-enabled deception that are particularly challenging for resource-constrained SMEs (Jabir et al., 2025). These developments reinforce the need for adaptive cyber exposure assessment frameworks capable of supporting continuous cyber resilience monitoring in rapidly evolving threat environments.

Nevertheless, most SME-focused cyber resilience studies remain conceptual or descriptive. They outline challenges, propose high-level frameworks, or discuss best practices, but rarely offer operational metrics that allow SMEs to measure, compare, and track their cyber resilience over time. This limitation directly constrains the practical usability of resilience concepts in SME decision-making.

2.2. Asset-based risk approaches

Asset-based risk assessment represents a significant methodological shift in cybersecurity research, emphasizing that cyber risks materialize through their impact on organizational assets rather than through technical vulnerabilities alone (Kure & Nwajana, 2022). This perspective aligns with risk management principles that prioritize the protection of assets critical to operational continuity, financial stability, and strategic objectives (Bahmanova & Lace, 2025a; 2025b; Sheffi, 2005).

The literature identifies a broad spectrum of SME-relevant assets, including information assets (customer data, financial records), IT infrastructure, operational processes, human capital, reputation, and increasingly, digital innovation assets such as AI systems and algorithmic models. Asset-based approaches highlight that cyber risks affect these assets unevenly, creating localized concentrations of exposure.

Previous studies, including the authors' own earlier work, have demonstrated the analytical value of mapping assets to cyber risk categories using matrix-based frameworks. Such matrices effectively visualize interdependencies and vulnerability patterns, making them particularly suitable for SMEs that require intuitive assessment tools.

However, despite their conceptual strength, asset-based models in the literature are predominantly qualitative. This approach lacks the capacity to quantify overall exposure, differentiate the relative importance of assets, support cross-organizational comparison, or guide resource allocation decisions.

Thus, while asset-based frameworks provide an essential foundation for understanding cyber exposure, they remain underutilized as decision-support instruments due to the absence of quantitative operationalization.

2.3. Quantitative cyber risk indices

Quantitative approaches to cyber risk and resilience measurement have been proposed across various domains, including information security, critical infrastructure protection, supply chain risk, and cyber-physical systems (Masud et al., 2025; Tsuji et al., 2023). These models commonly rely on combinations of likelihood-impact scoring, probabilistic modeling, multi-criteria decision-making (MCDM), and normalization techniques to construct indices or risk scores. Representative quantitative and sectoral cyber risk and resilience approaches that inform CREI's aggregation, normalization, and comparative logic span: attack-graph and threat-surface analytics and vulnerability assessment (Herranz-Oliveros et al., 2024; Zelle et al., 2022); explainable AI and security automation (Sarker et al., 2024; Muhammad et al., 2025); resilience modelling and risk-

informed decision methods in cyber-physical and critical infrastructure contexts (Cameron et al., 2019; Oughton et al., 2019; Veeramany et al., 2016; Fisher & Porod, 2023; Alshawish & de Meer, 2019); sector-specific risk assessment and threat management, including healthcare and automotive ecosystems (Huda et al., 2024; Silvestri et al., 2024; Pavão et al., 2024; Wai & Lee, 2023); blockchain and smart-contract related resilience and secure transaction models (Youssef & Boudriga, 2021; Guerreiro et al., 2017; Mustafa et al., 2023); and methodological treatments of resilience and high-impact disruptions (Strandberg et al., 2021; Rubakha & Tkachyk, 2024; Ribeiro et al., 2021). In addition, digital-asset protection and regulatory considerations provide practical grounding for SME-appropriate risk management practice (AllahRakha, 2024; Umunnakwe et al., 2021).

Such models contribute valuable methodological insights, particularly regarding weighting mechanisms, aggregation logic, and comparative analysis. However, when examined through an SME lens, several limitations become apparent.

First, many quantitative models require detailed historical incident data, loss statistics, or probability distributions that SMEs typically do not possess. Second, advanced techniques, such as stochastic simulations or attack graph analysis, often exceed the analytical capacity of SMEs and require expert facilitation. Third, numerous indices adopt a threat-centric or technical focus, neglecting organizational, human, and reputational dimensions that are critical for SMEs.

Moreover, existing indices rarely integrate asset criticality in a structured manner. Assets are often treated implicitly or uniformly, despite clear evidence that their importance varies significantly across SMEs and sectors. Similarly, while control maturity models are frequently discussed, their impact is usually represented qualitatively rather than as a quantifiable mitigating factor.

As a consequence, current quantitative cyber risk indices offer limited applicability for SMEs seeking simple, interpretable, and context-sensitive metrics that can inform strategic decision-making.

2.4. Research gap

The need for interpretable composite exposure metrics is also highlighted in risk quantification and operational resilience scholarship (Kopp et al., 2020; Ganin et al., 2016), and in foundational cyber resilience work that emphasizes adaptive capacity beyond prevention (Linkov & Kott, 2019; Linkov & Trump, 2019).

The synthesis of existing literature reveals a clear and persistent research gap at the intersection of cyber resilience, asset-based risk assessment, and quantitative measurement for SMEs.

First, although cyber resilience is widely recognized as essential for SMEs, there is a lack of quantitative, SME-oriented metrics capable of translating resilience concepts into actionable exposure scores. Second, asset-based frameworks effectively capture where cyber risks materialize but remain largely qualitative and non-operational. Third, quantitative cyber risk indices provide methodological rigor but are often incompatible with SME constraints, either due to complexity, data requirements, or insufficient integration of organizational assets.

Most importantly, the literature lacks a model that incorporates asset criticality and risk importance through structured weighting, integrates control maturity as a measurable mitigating factor, produces normalized scores suitable for benchmarking and longitudinal analysis, and remains usable under typical SME resource constraints.

This gap motivates the development of the CREI, which advances prior qualitative asset-risk mapping into a quantitative, decision-oriented metric. By positioning cyber risks as the primary driver and assets as the focal points of impact, the CREI responds directly to the limitations identified in existing research and provides a foundation for systematic measurement of SME cyber resilience.

3. Methodology

The methodological framework for the CREI builds upon the asset-risk matrix introduced in prior authors' research and extends it into a multidimensional framework capable of quantifying SME cyber exposure. While the earlier matrix provided a qualitative visualization of how critical assets intersect with major categories of cyber risks, the CREI transforms this conceptual foundation into a structured evaluation approach. This section outlines the methodological design of the CREI, including its conceptual structure, weighting logic, control maturity integration, and scoring principles, without introducing formal mathematical notation.

3.1. Overview of the prior asset-risk matrix

The asset-risk matrix underlying the CREI framework builds upon the authors' previously published research on SME critical assets and cyber risk typologies (Bahmanova & Lace, 2025a; 2025b), complemented by broader SME-focused cybersecurity literature and sectoral evidence (ENISA, 2021; 2023). The original framework identified seven categories of critical organizational assets and six major categories of cyber risks, capturing the qualitative relationships between them and providing a structured representation of cyber exposure within SME environments.

As a conceptual mapping instrument, the matrix facilitated the identification of asset-risk interactions and areas of concentrated vulnerability across organizational functions. However, its qualitative nature limited its applicability for comparative assessment, prioritization, and evidence-based decision-making. In particular, the framework did not incorporate risk likelihood, asset criticality differentiation, cybersecurity control maturity, or mechanisms for generating comparable quantitative exposure measures.

The CREI extends this foundational asset-risk structure by integrating these additional dimensions into a unified

assessment framework. By combining asset criticality, risk likelihood, risk importance, and control maturity within a quantitative aggregation process, the proposed approach transforms a qualitative representation of cyber exposure into a measurable, comparable, and decision-oriented cyber resilience assessment instrument.

3.2. Conceptual design of CREI

The CREI measures cyber exposure through the integration of five interrelated conceptual components, each reflecting insights from SME cybersecurity literature and prior qualitative analysis.

1. Likelihood of risk occurrence captures differences in how frequently risk categories materialize depending on sector dynamics, technologies used, and prevailing threat patterns.
2. Impact on critical assets represents the severity of consequences when a specific risk affects a specific asset, preserving the logic of the prior matrix while preparing it for quantitative aggregation.
3. Asset criticality acknowledges that not all SME assets contribute equally to resilience. For example, financial transactions may be more critical for fintech SMEs than operational workflows, requiring differentiated weighting.
4. Risk category importance reflects sector-specific threat landscapes and allows the model to be tailored while preserving cross-sector comparability.
5. Control maturity as a mitigating factor accounts for the strength of implemented controls, enabling the model to reflect realistic mitigation capacity rather than theoretical exposure alone.

Together, these components form the conceptual architecture of the CREI.

3.3. Weighting procedures (AHP and entropy)

Weighting constitutes a critical component of the CREI framework, as it enables the integration of heterogeneous dimensions, including organizational assets and cyber risk categories, into a unified exposure metric. To achieve both methodological rigor and practical applicability, CREI adopts a hybrid weighting approach that combines expert-informed and data-driven perspectives.

Expert-based weighting incorporates domain knowledge and contextual understanding, which is particularly important in SME environments where comprehensive cybersecurity datasets are often unavailable. At the same time, data-driven weighting methods, such as entropy analysis, enhance objectivity by capturing the variability and informational content of quantitative indicators when such data exist. The combination of these approaches allows the framework to balance expert judgment with statistical evidence, thereby reducing the limitations associated with relying exclusively on either subjective assessments or empirical observations.

Furthermore, the weighting structure is designed to accommodate sector-specific characteristics, enabling the relative importance of assets and cyber risk categories to reflect differences in industry contexts while preserving the overall consistency and comparability of the CREI framework. This hybrid weighting logic enhances both the robustness of the assessment process and the applicability of the model across SMEs with diverse operational environments and cyber exposure profiles.

3.4. Control maturity model

A distinguishing feature of the CREI framework is the explicit incorporation of cybersecurity control maturity as a core methodological dimension. Whereas many existing cyber risk assessment models primarily evaluate exposure through threat characteristics, vulnerabilities, or asset values, CREI integrates organizational mitigation capacity directly into the exposure calculation. This approach extends the assessment beyond traditional risk measurement by incorporating a resilience-oriented perspective that reflects an organization's ability to prevent, detect, respond to, and manage cyber incidents. Consequently, the framework captures not only the presence of cyber risks but also the effectiveness of organizational capabilities, including preventive controls, detection mechanisms, incident response preparedness, and the degree of process formalization and automation.

The maturity scale is designed specifically for SMEs, avoiding unnecessary complexity while retaining explanatory power. It acknowledges structural barriers faced by SMEs in implementing advanced controls and enables a realistic representation of their mitigation capacity.

3.5. Normalization and scoring

The CREI generates a normalized exposure score ranging from 0 to 100, designed to provide a transparent and interpretable representation of organizational cyber exposure. The scoring framework is based on the cumulative aggregation of exposure across all asset-risk interactions, thereby capturing the combined effect of cyber risks on critical organizational assets. To facilitate comparability across organizations, sectors, and assessment contexts, the aggregated exposure value is normalized against a theoretical maximum exposure level. The resulting index is interpreted through an inverse relationship between exposure and resilience: lower CREI values indicate lower cyber exposure and, consequently, higher levels of cyber resilience, whereas higher values reflect greater exposure and lower resilience.

By conceptualizing cyber resilience through the lens of exposure reduction, the CREI provides a practical and decision-oriented assessment framework that supports risk prioritization, resource allocation, and longitudinal monitoring. This exposure-based perspective also establishes the foundation for the mathematical formulation of the index presented in the subsequent section.

4. Model development

This section presents the development of the CREI. The model is designed to quantify the level of cyber exposure faced by SMEs by integrating cyber risks, critical assets, and organizational mitigation capabilities into a single structured framework.

The development of the CREI follows a stepwise logic. First, the mathematical structure of the index is defined. Second, the data required to operationalize the model are specified. Finally, sensitivity analysis is introduced to assess the robustness of the model and the stability of its results.

4.1. Mathematical formulation

The CREI is based on the premise that cyber exposure arises from the interaction between assets, cyber risk categories, and organizational preparedness. Exposure is therefore modeled as a cumulative effect of multiple asset-risk combinations, adjusted by the likelihood of risks and the maturity of implemented controls.

4.1.1. Notation and definitions

Let:

$$A=\{a_1,a_2,\ldots,a_m\} \tag{1}$$

denote the set of critical assets, where m = 7.

$$R=\{r_1,r_2,\ldots,r_n\} \tag{2}$$

denote the set of cyber risks categories, where n = 6.

Each asset represents a category of resources essential for SME operations (e.g., data, systems, processes), while each risk category reflects a distinct type of cyber threat.

Let the matrix of asset-risk relationships be:

$$M=\left[I_{a,r}\right]_{m\times n}. \tag{3}$$

Each value represents the expected magnitude of impact if a particular risk manifests against a particular asset. $I_{a,r}\in[1,3]$ represent the impact of risk category r on asset a. Higher values indicate more severe consequences in case the risk materializes.

To account for heterogeneity among assets and risks, weighting factors are introduced:

$W_a\in(0,1)$ be the criticality weight for asset a, with

$$\sum_{a=1}^{m} W_a=1; \tag{4}$$

$W_r\in(0,1)$ be the weight of risk category r, with

$$\sum_{r=1}^{n} W_r=1. \tag{5}$$

Finally, organizational preparedness is incorporated through a control maturity factor C_r, defined for each risk category:

$$C_r\in\{1.0,0.7,0.4,0.2\}, \tag{6}$$

where the values correspond to the control maturity factor for risk r.

Lower values correspond to higher maturity and stronger mitigation measures. The notation and definitions introduced in this section provide the formal basis for the CREI framework and establish the relationships between assets, cyber risks, weighting factors, and organizational control maturity used in subsequent calculations.

4.1.2. Exposure function

The exposure associated with asset a under risk category r is defined as:

$$E_{a,r}=L_r\times I_{a,r}\times W_a\times W_r\times C_r. \tag{7}$$

This formulation reflects five interacting dimensions of cyber exposure:

- Likelihood L_r increases expected frequency.
- Impact $I_{a,r}$ magnifies severity.
- Asset weight W_a increases exposure for high-value or mission-critical assets.
- Risk weight W_r accounts for sectoral differences.
- Control maturity C_r acts as a mitigation factor, reducing exposure as cybersecurity capabilities and organizational preparedness improve.

The multiplicative structure ensures that exposure increases when risks are more likely, impacts are more severe, assets are critical, or controls are weak. By design, when controls are weak (e.g., C = 1.0), exposure is maximal; when controls are advanced (C = 0.2), exposure is significantly reduced.

4.1.3. Aggregation and normalization

Total raw exposure is the sum of all cell-level exposures:

$$CREI_{raw}=\sum_{a=1}^{m}\sum_{r=1}^{n} E_{a,r}. \tag{8}$$

This raw index is sector-specific and depends on the organization's internal configuration. To enable comparability across organizations, the index is normalized. The maximum theoretical exposure occurs when likelihood and impact are at their maximum levels and no effective controls are in place:

$$CREI_{\max}=\sum_{a=1}^{m}\sum_{r=1}^{n} 25W_aW_r. \tag{9}$$

Since the asset and risk weights are normalized to sum to unity, the double summation of weighted exposures simplifies to a constant maximum value:

$$CREI_{\max}=25. \tag{10}$$

The normalized Cyber Resilience Exposure Index is therefore defined as:

$$CREI=\frac{CREI_{raw}}{CREI_{\max}}\times 100. \tag{11}$$

The resulting index ranges from 0 (minimal exposure) to 100 (maximum theoretical exposure). The normalization procedure ensures comparability across organizations,

sectors, and assessment contexts by expressing exposure as a percentage of the maximum theoretical exposure level.

4.2. Data requirements

The CREI model is designed to operate with a combination of expert judgment, empirical evidence, and organizational self-assessment, making it suitable for SMEs with limited data availability.

Three main data groups are required:

1. Impact data: Impact scores $I_{a,r}$ are obtained through literature review, expert assessments, or structured workshops. These values capture how severely each risk affects specific assets.
2. Risk likelihood and weighting data: Likelihood values L_r and risk weights W_r are derived from sectoral reports, cyber incident statistics, and expert consensus. Asset weights W_a reflect the strategic importance of assets and are typically derived through expert-based methods.
3. Control maturity data: Control maturity factors C_r are assessed using audits, questionnaires, or maturity models. They represent the effectiveness of preventive, detective, and corrective cybersecurity measures.

To enhance methodological rigor, weights may be derived using analytic hierarchy process (AHP), entropy-based methods, or hybrid approaches that combine expert judgment with data-driven variability.

4.3. Weighting methods

4.3.1. AHP (Analytic Hierarchy Process)

The Analytic Hierarchy Process (AHP) is a widely used multi-criteria decision-making method that derives relative weights from expert judgments through pairwise comparisons. In the CREI framework, AHP is used to determine both asset criticality weights and cyber risk category weights, enabling the incorporation of expert knowledge into the exposure assessment process. Let $P=\left[p_{ij}\right]$ (12) denote a matrix of pairwise comparisons where:

- p_{ij} >1 means asset a_i is more important than a_j.
- p_{ij} =1 / p_{ji}.

Weights are obtained from the normalized eigenvector of P. The same applies for risk categories.

The use of AHP offers several advantages for SME cyber resilience assessment. It incorporates expert knowledge in situations where historical cybersecurity data may be limited, produces transparent and interpretable weighting structures, and enables sector-specific customization by reflecting the priorities and operational characteristics of different organizations. Consequently, AHP provides a practical mechanism for translating qualitative expert assessments into quantitative weights that can be integrated into the CREI framework.

4.3.2. Entropy weighting

Entropy weighting captures the degree of variability in quantitative metrics associated with assets or risks. In the context of weighting, entropy reflects the amount of information contained within a set of indicators. Indicators that exhibit greater variability across assets or risk categories provide more discriminatory information and therefore receive higher weights, whereas indicators with relatively uniform values contribute less information and receive lower weights. As a result, entropy weighting reduces reliance on subjective judgment and enables the weighting structure to reflect observable differences in the underlying data.

Let x_{ij} denote the value of indicator j for asset or risk i.

Normalized: $p_{ij}=\frac{x_{ij}}{\Sigma_i x_{ij}}$; (13)

Entropy: $e_j=-k\Sigma p_{ij}\ \ln p_{ij}$, (14)

where $k=1/\ln(m)$ or $1/\ln(n)$. (15)

Weight: $w_j=\frac{1-e_j}{\Sigma_{j=1}^{n}(1-e_j)}$. (16)

Entropy weighting offers several advantages within the CREI framework. As a data-driven method, it identifies indicators with greater informational content and assigns weights according to their observed variability. This approach complements expert-based assessments by reducing subjectivity and improving the objectivity of the weighting process when sufficient quantitative data are available.

In the context of CREI, entropy weighting may be applied using quantitative indicators derived from cybersecurity audits, vulnerability assessments, penetration testing results, incident logs, compliance assessments, employee awareness testing outcomes, or sectoral benchmarking reports. These indicators provide the variability required to calculate informational entropy and support more objective weight estimation. The specific indicators selected may vary depending on the SME's industry, cybersecurity maturity, and data collection capabilities.

Although entropy weighting improves objectivity by incorporating variability in quantitative indicators, many SMEs face significant limitations regarding the availability of structured cybersecurity data. Consequently, entropy weighting should be considered an optional enhancement rather than a mandatory component of the CREI framework. To address differences in cybersecurity data maturity, CREI supports a tiered implementation approach. In the initial stage, SMEs may rely exclusively on expert-based weighting methods such as AHP. As organizations accumulate cybersecurity-related data, including incident records, audit findings, vulnerability assessments, and security performance metrics, entropy weighting can be progressively introduced to complement expert judgment. At higher levels of cybersecurity maturity, organizations may

adopt a hybrid weighting approach that combines AHP and entropy methods. This staged implementation ensures that CREI remains applicable across different levels of SME cybersecurity maturity while maintaining methodological consistency and practical usability.

4.3.3. Hybrid weighting

To combine the advantages of expert-driven and data-driven weighting approaches, the CREI framework supports a hybrid weighting strategy. Hybrid weights are calculated as:

$$W = \alpha W_{AHP} + (1-\alpha) W_{ENT}, \quad (17)$$

where $\alpha \in [0.5, 0.8]$ is selected to preserve the dominant role of expert judgment while incorporating empirical information derived from quantitative indicators. Higher values of α place greater emphasis on expert assessments, whereas lower values increase the influence of entropy-based weighting. This flexibility allows organizations to adapt the weighting structure according to the availability and quality of cybersecurity data.

The hybrid approach is particularly relevant for SMEs that possess partial cybersecurity data but still rely heavily on expert knowledge. By combining subjective and objective weighting mechanisms, the approach reduces the limitations associated with using either method in isolation and provides a more balanced representation of asset criticality and cyber risk importance. Consequently, hybrid weighting serves as a practical bridge between expert-based assessment and data-driven decision-making within the CREI framework.

4.4. Control maturity scaling

The control maturity factor C_r is used to incorporate organizational preparedness and mitigation capability into the CREI framework. Unlike traditional cyber risk exposure models that focus primarily on likelihood and impact, the inclusion of C_r allows the framework to account for the effectiveness of cybersecurity controls, governance practices, employee awareness, incident response capabilities, and other resilience-enhancing measures.

The control maturity factor is defined as: $C_r \in \{1.0, 0.7, 0.4, 0.2\}$.

where higher values correspond to weaker control environments and lower levels of cybersecurity maturity, while lower values indicate stronger controls and greater resilience capacity. Under this scale, (C_r = 1.0) represents minimal mitigation capability, whereas (C_r = 0.2) reflects a highly mature control environment capable of substantially reducing cyber exposure.

By directly modifying exposure values, the control maturity factor transforms CREI from a purely exposure-oriented metric into a resilience-oriented assessment framework. This approach reflects the understanding that cyber resilience depends not only on the existence of threats and vulnerabilities but also on an organization's ability to prevent, withstand, respond to, recover from, and adapt to cyber incidents.

The maturity levels should be determined through expert assessment, cybersecurity audits, compliance reviews, or other organizational evaluation mechanisms. While a common scaling structure is proposed in this study, future research may develop risk-specific maturity scales to better reflect differences in mitigation effectiveness across cyber risk categories. For example, certain risks, such as social engineering and insider-related threats, may require alternative scaling approaches due to their stronger dependence on human behaviour and organizational culture.

4.5. CREI calculation workflow and robustness considerations

The robustness of the CREI framework is supported by its transparent structure and by the ability to examine how variations in key input parameters influence the final exposure score. In the present framework, robustness considerations focus on asset weights, risk weights, likelihood scores, and control maturity factors, as these parameters directly affect exposure estimation and prioritization outcomes. Since asset criticality, risk relevance, and organizational preparedness may differ across sectors and organizational contexts, the influence of individual parameters should be interpreted within the specific assessment environment. This approach supports scenario based analysis and allows users to evaluate the stability of results under alternative assumptions. Figure 1 presents the methodological workflow used to calculate and interpret the Cyber Resilience Exposure Index.

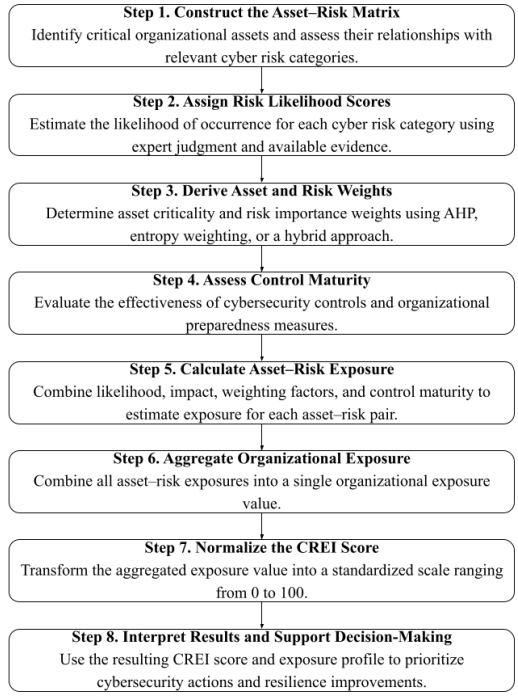


Figure 1. Methodological workflow for CREI calculation and interpretation

The workflow begins with the identification of critical organizational assets and relevant cyber risk categories. Likelihood values, weighting factors, and control maturity levels are subsequently assigned and combined to calculate exposure values for individual asset risk combinations. These values are aggregated and normalized to generate the final CREI score, which can then be used to support cybersecurity prioritization, resource allocation, benchmarking, and periodic reassessment activities.

The mathematical formulation of CREI is designed to balance analytical rigor with practical interpretability. Each component of the model, including risk likelihood, impact severity, asset criticality, risk weighting, and control maturity, has a clearly defined conceptual role. This allows the final exposure score to be traced back to specific organizational and risk related factors. At the same time, the framework remains adaptable across sectors because weights and likelihood values can be adjusted to reflect different operational contexts without altering the underlying structure of the index. By transforming qualitative expert judgments into normalized quantitative values, CREI supports systematic exposure assessment while avoiding the complexity of highly data intensive probabilistic models. This formalization provides the methodological foundation for the illustrative application presented in the following section.

5. Illustrative example

This section presents an illustrative application of the CREI to a hypothetical SME. The purpose of the example is to demonstrate how the proposed model operates in practice, how input parameters are combined, and how the resulting index can be interpreted for managerial decision-making. The example is sector-realistic but not company-specific. All values are either adopted from prior research or synthetically constructed based on typical conditions described in the literature, ensuring transparency while preserving confidentiality.

5.1. Introduced SME sector

The illustrative example considers an SME operating in the financial sector, such as a small payment service provider or a FinTech organization. The financial sector was selected because of its strong dependence on digital assets, information systems, and technology-enabled service delivery, which collectively increase exposure to cyber threats. In addition, financial-sector SMEs are frequently targeted by cyberattacks, including phishing campaigns, malware infections, data breaches, and cyber-enabled fraud, making cybersecurity and resilience particularly critical in this context.

A further rationale for this sectoral focus is methodological consistency. The asset-risk impact matrix applied in the illustrative example is derived from the authors' previous research, in which cyber risks and their impacts were evaluated by experts specifically within the context of financial-sector SMEs. Consequently, the example maintains continuity with the underlying qualitative framework while demonstrating its extension into a quantitative cyber exposure assessment model.

5.2. Input values

5.2.1. Assets and asset weights

The example uses the same seven asset categories as defined in the previous study:

1. Customer and Client Data (CD)
2. Operational and Business Processes (OP)
3. IT Infrastructure and Digital Systems (IT)
4. Employee Knowledge and Human Capital (HC)
5. Brand and Reputation (BR)
6. Artificial Intelligence Systems and Algorithms (AI)
7. Financial Assets and Transactions (FA)

To reflect the relative importance of different organizational assets in a financial-sector SME, asset criticality weights W_a were assigned such that their sum equals 1.0. These weights represent the contribution of each asset category to overall cyber exposure and serve as an input parameter in the CREI calculation. The assumed asset weights used in the illustrative example are presented in Table 1.

Table 1. Assumed asset criticality weights for the illustrative financial-sector SME

Asset	Description	Weight W_a
CD	Customer and client data	0.20
OP	Operational and business processes	0.05
IT	IT infrastructure and digital systems	0.15
HC	Employee knowledge and human capital	0.10
BR	Brand and reputation	0.15
AI	AI systems and algorithms	0.15
FA	Financial assets and transactions	0.20

These weights reflect the results of the prior qualitative analysis, where customer data and financial transactions were identified as the most critical assets, followed by IT systems, AI components, and organizational reputation.

5.2.2. Risk categories, likelihood, and risk weights

The same six cyber risk categories are retained:

1. External Threats and Cyberattacks (Ext)
2. Insider and Human-related Risks (Ins)
3. Data Vulnerabilities and Information Security Risks (Data)
4. Reputational and Financial Risks (RepFin)
5. Emerging and Advanced Cyber Threats (Emerg)
6. Operational and Technological Weaknesses (Oper)

Likelihood scores L_r were assigned to each cyber risk category using a five-point ordinal scale, where higher values indicate a greater expected frequency of occurrence. The assessment reflects common threat patterns observed in financial-sector SMEs and serves as an input parameter

for the CREI calculation. The assumed likelihood scores used in the illustrative example are presented in Table 2.

Table 2. Assumed likelihood scores for cyber Risk Categories in the illustrative financial-sector SME

Risk	Description	Likelihood L_r
Ext	External attacks (malware, phishing, etc.)	5
Ins	Insider misuse, social engineering	3
Data	Data vulnerabilities and breaches	4
RepFin	Reputational and financial consequences	4
Emerg	AI-enabled, deepfake, advanced threats	4
Oper	Operational and technological weaknesses	3

Risk category weights W_r were assigned to capture the relative importance of each cyber risk category in the context of a financial-sector SME. The weights were normalized such that their sum equals 1.0 and serve as an input parameter in the CREI computation. The assumed risk weights used in the illustrative example are presented in Table 3.

Table 3. Assumed risk category weights for the illustrative financial-sector SME

Risk	Weight W_r
Ext	0.25
Ins	0.10
Data	0.20
RepFin	0.20
Emerg	0.15
Oper	0.10

External attacks, data-related risks, and reputational/financial risks receive higher weights, consistent with empirical evidence from financial-sector cybersecurity studies.

5.2.3. Control maturity levels

Control maturity is assessed per risk category using the four-level scale defined in the model:

- Level 1: Ad-hoc or nonexistent controls → factor 1.0
- Level 2: Basic controls → factor 0.7
- Level 3: Managed controls → factor 0.4
- Level 4: Optimized controls → factor 0.2

Control maturity levels were assigned for each cyber risk category to reflect the typical cybersecurity posture of a financial-sector SME. The assumed maturity levels and corresponding mitigation factors (C_r) are presented in Table 4.

These assumptions reflect a typical financial SME with relatively stronger defenses against common external threats and weaker preparedness for insider-related and emerging risks.

Table 4. Assumed control maturity levels and mitigation factors by cyber risk category

Risk	Qualitative maturity level	Factor C_r
Ext	Basic-managed controls	0.7
Ins	Ad-hoc controls	1.0
Data	Basic controls	0.7
RepFin	Basic controls	0.7
Emerg	No dedicated controls	1.0
Oper	Basic controls	0.7

5.2.4. Impact matrix

Impact values $I_{a,r}$ are directly adopted from the previously published asset-risk matrix for financial-sector SMEs. The scale ranges from 1 (low impact) to 3 (high impact), and all values remain unchanged to ensure methodological continuity.

For example:

- Customer and Client Data is highly affected by external attacks, data vulnerabilities, and reputational/financial risks.
- IT Infrastructure shows high impact from external, data-related, emerging, and operational risks.
- Financial Assets and Transactions are strongly affected by external, data, and financial risks.

In the article, the full matrix is either referenced from the prior publication or reproduced as a separate table.

5.3. Calculation

Using the exposure function previously defined in Equation (7), exposure is calculated for each asset-risk pair.

$$E_{a,r} = L_r \times I_{a,r} \times W_a \times W_r \times C_r .$$

To illustrate the calculation, consider the following example:

- Asset: Customer and Client Data (CD)
- Risk: External Threats (Ext)

Input values:

- $L_{Ext} = 5$
- $I_{CD,Ext} = 3$
- $W_{CD} = 0.20$
- $W_{Ext} = 0.25$
- $C_{Ext} = 0.7$

The exposure value is therefore:

$$E_{a,r} = 5 \times 3 \times 0.20 \times 0.25 \times 0.7 = 0.252 .$$

The same procedure is applied to all 42 asset-risk combinations (7 assets × 6 risks). Summing all exposure values yields the raw index:

$$CREI_{raw} = 7.68.$$

The normalized CREI score is calculated using the maximum theoretical exposure defined in Equations (9) and (10), following the normalization procedure presented in Equation (11).

$$CREI = \frac{7.68}{25} \times 100 = 30.7.$$

5.4. Interpretation

A CREI score of approximately 31 out of 100 indicates relatively low overall cyber exposure and, consequently, comparatively high cyber resilience under the assumed conditions.

To support interpretation, exposure can be decomposed by assets and by risk categories.

By asset, the highest exposure contributions come from:

- Customer and Client Data,
- Financial Assets and Transactions,
- IT Infrastructure and Brand/Reputation.

By risk category, the dominant exposure drivers are:

- External Threats,
- Data Vulnerabilities,
- Reputational and Financial Risks.

Although insider and operational risks show lower numerical contributions, their impact remains non-negligible, particularly given weaker control maturity. Emerging threats already contribute substantially despite their relatively recent appearance, highlighting future risk potential.

Overall, the illustrative example demonstrates that the CREI:

- quantifies overall cyber exposure,
- identifies where exposure is concentrated,
- supports SMEs in prioritizing cybersecurity investments under resource constraints.

In future research, the model can be applied to real-world SME samples to enable benchmarking, comparative analysis, and empirical validation of weighting and maturity assumptions.

Sensitivity analysis indicated that the control maturity factor exerted the strongest influence on the final CREI score among the examined parameters. Variations in control maturity produced larger changes in overall exposure than comparable adjustments in asset weights or individual likelihood scores. This result reflects the multiplicative structure of the model, where control maturity directly affects exposure across all asset-risk combinations associated with a given risk category.

The findings suggest that improvements in cybersecurity controls, governance practices, employee awareness programs, and incident response capabilities can generate a greater reduction in overall exposure than isolated changes in asset prioritization. Asset criticality weights and risk likelihood values also influenced the final score, but their impact was comparatively moderate. Consequently, the analysis highlights control maturity as the primary leverage point for reducing cyber exposure and strengthening cyber resilience in SMEs.

5.5. Limitations of the illustrative example

The illustrative example is synthetic and not based on a specific SME, as all input parameters are sector-informed and introduced solely to demonstrate the functioning of the CREI model. Impact values are adopted from prior qualitative research, while likelihoods, weights, and control maturity levels rely on expert-informed assumptions rather than firm-level empirical data. Consequently, the numerical results should not be interpreted as representative of any individual organization. The example assumes static parameter values and does not capture temporal changes in risk exposure or control maturity. In addition, interdependencies and cascading effects between cyber risks and assets are not explicitly modeled. Finally, the example focuses on a single sector, and application to other sectors would require recalibration of model parameters. Despite these limitations, the example effectively illustrates the logic, transparency, and interpretability of the CREI framework.

6. Results and discussion

This section presents and discusses the results obtained from applying the CREI. The discussion focuses on the interpretation of the results, their methodological and practical relevance, and the positioning of the proposed framework within the broader landscape of cyber risk and resilience assessment approaches for SMEs. Given the illustrative and methodological nature of the study, the discussion emphasizes conceptual comparison and analytical contribution rather than direct numerical comparison with prior empirical studies.

6.1. Summary of key results

The illustrative application of the CREI model results in a normalized exposure score of approximately 31 out of 100 for a representative financial-sector SME. This value reflects a relatively low level of overall cyber exposure under the assumed conditions and, consequently, a comparatively high level of cyber resilience. More importantly than the absolute value, the decomposition of exposure reveals how cyber risks are distributed across assets and risk categories. The results indicate that exposure is concentrated in a limited number of critical assets – most notably customer and client data, financial assets and transactions, IT infrastructure, and organizational reputation. From a risk perspective, external cyberattacks, data-related risks, and reputational and financial risks emerge as the dominant contributors to total exposure. These findings confirm that cyber exposure in SMEs is not evenly distributed, but instead driven by specific asset-risk combinations.

Sensitivity testing indicated that control maturity exerted the strongest influence on the final CREI score. A one-level improvement in control maturity reduced total exposure by approximately 15–25%, depending on the risk category. Changes in asset weights produced moderate effects, while variations in individual likelihood scores had a smaller impact on overall exposure. This finding highlights the strategic importance of investing in cybersecurity controls, governance mechanisms, and employee awareness programs.

6.2. Interpretation of CREI as a cyber resilience indicator

The CREI score should be interpreted as a relative exposure indicator, not as an absolute measure of security or insecurity. A lower CREI value indicates that, given the organization's asset structure, risk environment, and control maturity, the expected cyber exposure is limited. In this context, a CREI score of approximately 31 suggests that the illustrative SME benefits from a certain degree of resilience, primarily due to non-maximal control maturity against high-likelihood risks. However, the index simultaneously reveals residual exposure, particularly in areas where controls are weak or risks are emerging. The CREI thus operationalizes cyber resilience not as a binary state, but as a continuum shaped by likelihood, impact, criticality, and mitigation. This interpretation aligns with contemporary views of resilience as an adaptive and dynamic capability rather than a static condition.

6.3. Comparison with existing cyber risk and resilience approaches

Rather than aiming to directly compare empirical results with prior studies, this section positions the CREI within the broader family of cyber risk and resilience assessment approaches. Compared to traditional cybersecurity assessment tools, the CREI offers several distinctive features. Unlike checklist-based assessments and maturity models, it produces a quantitative exposure score while preserving interpretability, as each component of the index has a clear conceptual meaning and can be traced back to specific drivers, which aligns with broader management research emphasizing interpretable, decision-oriented risk metrics (Kopp et al., 2020; Kliestik et al., 2020). In contrast to conventional risk matrices that rely on unweighted likelihood-impact combinations, the CREI explicitly integrates asset criticality, cyber risk importance, and control maturity into a single coherent formulation. This logic is consistent with multi-criteria and composite assessment approaches used in business risk and performance analysis, where weighting and prioritization are central to managerial decision-making under uncertainty (Virglerova et al., 2021). This enables a more nuanced differentiation between risks that are frequent but well controlled and those that are less frequent but insufficiently mitigated. Moreover, while many existing frameworks conceptualize cyber resilience qualitatively, the CREI operationalizes resilience through exposure reduction, enabling structured benchmarking across organizations, sectors, or time periods, as increasingly advocated in resilience-oriented risk management literature (Linkov & Kott, 2019). In this sense, the CREI complements rather than replaces existing approaches, serving as a bridge between qualitative expert judgment and quantitative decision support.

6.4. Managerial and practical implications for SMEs

From a managerial perspective, the CREI framework provides practical value by enabling SMEs to prioritize cybersecurity investments in a targeted and resource-efficient manner. By identifying which assets and cyber risk categories contribute most to overall exposure, the index allows decision-makers to move beyond uniform risk reduction and instead focus limited resources on areas with the highest marginal impact. The explicit integration of control maturity further highlights leverage points where improvements in governance, employee training, or technical safeguards can significantly reduce exposure, for example by strengthening defenses against prevalent external threats or enhancing data protection practices. In addition, the decomposition of the CREI supports communication with key stakeholders, including management, regulators, and business partners, by translating complex cyber risk landscapes into an interpretable exposure score and a structured breakdown of underlying drivers. Overall, the CREI is particularly well suited to SMEs, where cybersecurity decisions must be made under conditions of limited data availability, expertise, and financial capacity.

To maintain decision relevance, SMEs should reassess their CREI on a regular basis. Under normal operating conditions, a semi-annual reassessment is recommended. However, recalculation should also be triggered by significant organizational or technological changes, including cloud migration, deployment of AI systems, mergers, introduction of remote work practices, or major cybersecurity incidents. In highly regulated or threat-intensive sectors such as finance and healthcare, quarterly reassessment may provide additional benefits.

6.5. Methodological contributions

From a methodological standpoint, this study contributes to the cyber resilience literature by introducing a formalized exposure-based operationalization of cyber resilience that integrates assets, cyber risks, and mitigation controls within a unified mathematical framework. The model demonstrates how qualitative expert assessments can be systematically transformed into quantitative indicators without sacrificing interpretability, thereby bridging the gap between descriptive risk analysis and decision-oriented measurement. By normalizing exposure values, the CREI enables meaningful comparison across organizations, sectors, and time periods, addressing a common limitation of firm-specific cyber risk assessments. Taken together, these contributions position the CREI as a flexible methodological tool that supports both academic analysis and applied cybersecurity management.

6.6. Robustness and applicability

The robustness of the CREI framework is supported by its transparent structure, which enables the influence of key

parameters on overall cyber exposure to be systematically examined and interpreted. This transparency allows practitioners to adapt model assumptions to different organizational and sectoral contexts while maintaining methodological consistency. At the same time, the results should be interpreted within the scope of the framework and the assumptions underlying the illustrative example.

The influence of individual CREI parameters is expected to vary across sectors and organizational environments. Previous research has shown that SMEs operating in different industries exhibit distinct combinations of critical assets, cyber risks, and resilience capabilities due to variations in business models, digital dependencies, operational processes, and stakeholder relationships (Bahmanova & Lace, 2026a; 2026b). Consequently, no single parameter can be assumed to be universally dominant across all SME contexts. Nevertheless, the control maturity factor C_r occupies a distinctive position within the CREI framework because it represents the resilience dimension of cyber risk assessment. Unlike conventional exposure models that primarily focus on likelihood and impact, CREI incorporates organizational preparedness through cybersecurity controls, governance practices, employee awareness, and incident response capabilities. The inclusion of C_r therefore enables the framework to capture mitigation capacity alongside exposure, reflecting the broader cyber resilience perspective that emphasizes the ability to withstand, respond to, recover from, and adapt to cyber disruptions.

An additional limitation of the current CREI formulation concerns the assumption of independence between asset-risk pairs. The model evaluates each asset-risk interaction separately and aggregates exposure through a linear additive structure. While this approach enhances transparency, interpretability, and ease of implementation for SMEs, it does not fully capture the systemic nature of cyber incidents and the interdependencies that often exist between organizational assets.

In practice, cyber events frequently generate cascading effects across multiple assets and business functions. For example, a successful compromise of IT infrastructure may simultaneously result in customer data exposure, operational disruption, financial losses, regulatory consequences, and reputational damage. Similarly, a data breach may trigger secondary effects that extend beyond the initially affected asset category, influencing customer trust, business continuity, and long-term organizational performance.

Consequently, the current version of CREI should be interpreted as a first-order exposure assessment model that captures direct asset-risk relationships rather than higher-order interdependencies. The illustrative example presented in this study is intentionally static and sector-specific, serving to demonstrate the applicability of the framework rather than to provide universally generalizable exposure values. Future research should focus on empirical validation across multiple industries and organizational contexts, as well as on extending the framework through dependency matrices, network-based modelling, system dynamics approaches, or Bayesian structures capable of representing cascading and compound cyber impacts across interconnected organizational assets.

6.7. Addressing the research questions

The findings of this study provide clear responses to the research questions formulated in the introduction and further demonstrate the practical value of the proposed CREI framework.

With regard to the first research question, the literature review and the illustrative application of the model indicate that cyber exposure in SMEs is concentrated around a limited number of critical assets and cyber risk categories. Customer and client data, financial assets and transactions, IT infrastructure, and organizational reputation emerged as the most influential assets due to their direct contribution to business continuity, financial stability, and stakeholder trust. From the risk perspective, external cyberattacks, data vulnerabilities, and reputational-financial risks generated the largest contribution to overall exposure. These findings confirm that cyber exposure is not uniformly distributed across organizational assets and cyber risk categories, thereby supporting the asset-risk matrix logic underlying the CREI framework.

The second research question concerned the integration of asset criticality, cyber risk likelihood, and cybersecurity control maturity into a unified quantitative assessment approach. The proposed Cyber Resilience Exposure Index addresses this challenge by combining likelihood, impact severity, asset weights, risk weights, and control maturity factors within a single mathematical formulation. The resulting exposure score transforms qualitative assessments into a normalized quantitative indicator ranging from 0 to 100, enabling systematic aggregation, comparison, and interpretation of cyber exposure across organizations and sectors.

Finally, the third research question focused on the practical applicability of the framework for resource-constrained SMEs. The results demonstrate that CREI can support managerial decision-making by identifying the specific asset-risk combinations that contribute most significantly to overall cyber exposure. This decomposition enables organizations to prioritize cybersecurity investments, governance improvements, employee awareness initiatives, and technical controls according to their expected exposure reduction potential. By translating complex cyber risk relationships into an interpretable numerical score and exposure profile, the framework provides a practical decision-support mechanism that aligns cybersecurity priorities with SME resource constraints and resilience objectives.

7. Conclusions and future research

The literature review demonstrated that existing approaches to cyber resilience assessment in SMEs remain

fragmented across qualitative frameworks, asset-risk matrices, and quantitative risk evaluation models. While many studies emphasize the importance of identifying critical assets and cyber risks, relatively few provide practical mechanisms for transforming qualitative assessments into decision-oriented quantitative indicators suitable for resource-constrained organizations. This gap provided the primary motivation for the development of the CREI.

This paper proposed the CREI as a quantitative framework for assessing cyber risk exposure, where lower exposure reflects higher cyber resilience. The model integrates cyber risk likelihood, impact severity, asset criticality, risk importance, and control maturity into a single interpretable indicator, operationalizing cyber resilience as exposure reduction rather than a binary condition.

The findings provide clear responses to the research questions formulated in the study. The results indicate that cyber exposure in SMEs is concentrated around a limited number of critical assets and risk categories, that these dimensions can be integrated into a unified quantitative exposure metric, and that the resulting indicator can support cybersecurity prioritization and resource allocation decisions under SME resource constraints.

The study's main contribution lies in the formalization of a transparent exposure-based approach that transforms qualitative expert judgments into a structured quantitative assessment. The illustrative example demonstrated how CREI enables the decomposition of cyber exposure across assets and risk categories, thereby supporting targeted interpretation and prioritization of cybersecurity efforts in resource-constrained SMEs.

While the illustrative application is synthetic, it highlights the analytical value of the framework and its potential for practical decision support. Future research should focus on empirical validation of the CREI using real-world SME data, sector-specific calibration of model parameters, and extensions toward dynamic and interdependent risk modelling. Future developments of the CREI framework should focus on incorporating asset interdependencies, cascading cyber impacts, and dynamic exposure propagation mechanisms to better represent the systemic nature of contemporary cyber threats, including AI-enabled attack scenarios. To maintain decision relevance, organizations applying CREI should perform periodic reassessments, with semi-annual reviews recommended under normal operating conditions and more frequent updates following significant technological, organizational, or threat-related changes. Such extensions would further strengthen the applicability of the framework and support its use as a continuous cyber resilience monitoring and decision-support instrument.

AI Acknowledgements

ChatGPT (OpenAI, GPT-5.2, GPT-6) were used exclusively to support English language editing and stylistic refinement. The authors retain full responsibility for the scientific content, methodology, analysis, interpretation, and conclusions presented in this paper.

References

Al-Hawamleh, A. M. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems*, *15*(1), 1315–1331. https://doi.org/10.12785/ijcds/150193

AllahRakha, N. (2024). Cybersecurity regulations for protection and safeguarding digital assets (data) in today's worlds. *Lex Scientia Law Review*, *8*(1), 405–432. https://doi.org/10.15294/lslr.v8i1.2081

Alshawish, A., & de Meer, H. (2019). Risk mitigation in electric power systems: Where to start? *Energy Informatics*, *2*, Article 34. https://doi.org/10.1186/s42162-019-0099-6

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, *253*(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Aven, T., & Zio, E. (2018). Foundational aspects of risk assessment and risk management. *Risk Analysis*, *38*(1), 1–7.

Bahmanova, A., & Lace, N. (2025a). Aligning SME critical assets with cyber risks using a matrix model to develop a cyber resilience framework. *Journal of Systemics, Cybernetics and Informatics*, *23*(5), 11–16. https://doi.org/10.54808/JSCI.23.05.11

Bahmanova, A., & Lace, N. (2025b). Types of cyber risks for SMEs: Classification and business impact. In V. Davidavičienė, V. Skvarciany, & K. Peleckis (Eds.), *Selected Proceedings of the 15th International Scientific Conference "Business and Management 2025"* (pp. 484–491). Vilnius Gediminas Technical University. https://doi.org/10.3846/bm.2025.1556

Bahmanova, A., & Lace, N. (2026a). Key factors shaping collaborative cyber resilience in SMEs through open innovation. *Journal of Open Innovation: Technology, Market, and Complexity*, *12*(1), Article 100715. https://doi.org/10.1016/j.joitmc.2026.100715

Bahmanova, A., & Lace, N. (2026b). Modelling cyber resilience in SMEs as a socio-technical system: A systemic approach to adaptive digital risk management. *Systems*, *14*(2), Article 151. https://doi.org/10.3390/systems14020151

Cameron, C., Patsios, C., Taylor, P. C., & Pourmirza, Z. (2019). Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes. *IEEE Transactions on Smart Grid*, *10*(3), 3010–3019. https://doi.org/10.1109/TSG.2018.2817046

Dhanushkodi, K., & Thejas, S. (2024). AI enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. *IEEE Access*, *12*, 173127–173136. https://doi.org/10.1109/ACCESS.2024.3493957

Duraj, B., Tola, I., & Poshnjari, P., & Perri, R. (2025). Probability of bank distress: Investigating a risk landscape of an emerging economy. *Risk Governance and Control: Financial Markets & Institutions*, *15*(1), 119–129. https://doi.org/10.22495/rgcv15i1p12

European Union Agency for Cybersecurity. (2021). *Cybersecurity for SMEs: Challenges and recommendations*. Publications Office of the European Union.

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. Publications Office of the European Union. https://doi.org/10.2824/782573

Fisher, R. E., & Porod, C. H. (2023). Enhancing resilience of our Nation's critical infrastructure. In C. Smith, S. Prescott, & Z. Ma (Eds.), *Risk-informed methods and applications in nuclear and*

energy engineering: *Modeling, experimentation, and validation* (pp. 205–216). Academic Press. https://doi.org/10.1016/B978-0-323-91152-8.00002-8

Ganin, A. A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J. M., Kott, A., Mangoubi, R., & Linkov, I. (2016). Operational resilience: Concepts, design and analysis. *Scientific Reports*, *6*, Article 19540. https://doi.org/10.1038/srep19540

Guerreiro, S., Guédria, W., Lagerström, R., & Van Kervel, S. J. H. (2017). A meta model for interoperability of secure business transactions – using blockchain and DEMO. In *Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management* (*KEOD 2017*) (pp. 253–260). SciTePress. https://doi.org/10.5220/0006517502530260

Herranz-Oliveros, D., Tejedor-Romero, M., Gimenez-Guzman, J. M., & Cruz-Piris, L. (2024). Unsupervised learning for lateral-movement-based threat mitigation in active directory attack graphs. *Electronics*, *13*(19), Article 3944. https://doi.org/10.3390/electronics13193944

Huda, S., Islam, M. R., Abawajy, J., Kottala, V. N. V., & Ahmad, S. (2024). A cyber risk assessment approach to federated identity management framework-based digital healthcare system. *Sensors*, 24(16), Article 5282. https://doi.org/10.3390/s24165282

Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *Open Access Research Journal of Science and Technology*, *11*, 1–4. https://doi.org/10.53022/oarjst.2024.11.1.0060

Jabir, R., Le, J., & Nguyen, C. (2025). Phishing attacks in the age of generative artificial intelligence: A systematic review of human factors. *AI 2025*, *6*(8), Article 174. https://doi.org/10.3390/ai6080174

Kliestik, T., Valaskova, K., Lazaroiu, G., Kovacova, M., & Vrbka, J. (2020). Remaining financially healthy and competitive: The role of financial predictors. *Journal of Competitiveness*, *12*(1), 74–92. https://doi.org/10.7441/joc.2020.01.05

Kopp, E., Kaffenberger, L., & Wilson, C. (2020). *Cyber risk measurement*: *Towards a manageable approach* (IMF Working Paper No. 2020/149). International Monetary Fund.

Kure, H. I., & Nwajana, A. O. (2022). Protection of critical infrastructure using an integrated cybersecurity risk management (i-CSRM) framework. In *5G Internet of Things and changing standards for computing and electronic systems* (pp. 94–133). IGI Global. https://doi.org/10.4018/978-1-6684-3855-8.ch004

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In A. Kott & I. Linkov (Eds), *Cyber resilience of systems and networks*. *Risk, systems and decisions*. Springer. https://doi.org/10.1007/978-3-319-77492-3_1

Linkov, I., & Trump, B. D. (2019). *The science and practice of resilience*. Springer. https://doi.org/10.1007/978-3-030-04565-4

Masud, M. T., Keshk, M., Moustafa, N., Turnbull, B., & Susilo, W. (2025). Vulnerability defence using hybrid moving target defence in Internet of Things systems. *Computers & Security*, *153*, Article 104380. https://doi.org/10.1016/j.cose.2025.104380

Muhammad, A. H., Nasiri, A., & Harimurti, A. (2025). Machine learning methods for classification and prediction information security risk assessment. *IAES International Journal of Artificial Intelligence*, *14*(1), 457–465. https://doi.org/10.11591/ijai.v14.i1.pp457-465

Mustafa, I., McGibney, A., & Rea, S. (2023). Smart contract life-cycle management: An engineering framework for the generation of robust and verifiable smart contracts. *Frontiers in Blockchain*, *6*, Article 1276233. https://doi.org/10.3389/fbloc.2023.1276233

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce.

Oughton, E. J., Ralph, D., Pant, R., Leverett, E., Copic, J., Thacker, S., Dada, R., Ruffle, S., Tuveson, M., & Hall, J. W. (2019). Stochastic counterfactual risk analysis for the vulnerability assessment of cyber-physical attacks on electricity distribution infrastructure networks. *Risk Analysis*, *39*(9), 2012–2031. https://doi.org/10.1111/risa.13291

Pavão, J., Bastardo, R., & Rocha, N. P. (2024). Cyber resilience and healthcare information systems, a systematic review. *Procedia Computer Science*, *239*, 149–157. https://doi.org/10.1016/j.procs.2024.06.157

Radanliev, P., De Roure, D. C., Page, K., Nurse, J. R. C., Mantilla Montalvo, R., Santos, O., Maddox, L., & Burnap, P. (2020). Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and Industry 4.0 supply chains. *Cybersecurity*, *3*(1), Article 13. https://doi.org/10.1186/s42400-020-00052-8

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, *27*(2–3), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Rea-Guaman, M., Calvo-Manzano, J. A., & Feliu, T. S. (2018). A prototype to manage cybersecurity in small companies. In *2018 13th Iberian Conference on Information Systems and Technologies* (*CISTI*) (pp. 1–6). IEEE. https://doi.org/10.23919/CISTI.2018.8399252

Ribeiro, D., Almeida, A., Azevedo, A., & Ferreira, F. (2021, 7–10 September). Resilience in Industry 4.0 digital infrastructures and platforms. In *Advances in Manufacturing Technology XXXIV*: *Proceedings of the 18th International Conference on Manufacturing Research, incorporating the 35th National Conference on Manufacturing Research*, University of Derby, Derby, UK (pp. 390–395). SAGE Publications. https://doi.org/10.3233/ATDE210067

Rubakha, M., & Tkachyk, F., Pryimak, I., Demchyshak, N., & Yurkiv, R. (2024). Factor analysis of financial performance and formation of strategic resilience in Ukrainian IT companies under the challenges of war. *Financial and Credit Activity*: *Problems of Theory and Practice*, *1*(54), 260–281. https://doi.org/10.55643/fcaptp.1.54.2024.4229

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023a). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors*, *23*(15), Article 6666. https://doi.org/10.3390/s23156666

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023b). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, *23*(16), Article 7273. https://doi.org/10.3390/s23167273

Sarker, I. H., Janicke, H., Mohsin, A., Gill, A., & Maglaras, L. (2024). Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. *ICT Express*, *10*(4), 935–958. https://doi.org/10.1016/j.icte.2024.05.007

Sarfraz, M., Sumra, I. A., Khalid, B., & Fatima, E. (2025). AI-driven predictive threat detection and cyber risk mitigation: A survey. *Journal of Computing & Biomedical Informatics*, *8*(02).

Shafiq, M., Awan, M., Alwageed, H. S., Hassan, M. M., & Khan, R. A. (2026). *AI-driven agentic framework for insider threats prevention and detection in secure software development organizations*: *A fuzzy AHP approach*. Research Square. https://doi.org/10.21203/rs.3.rs-8756821/v1

Sheffi, Y. (2005). *The resilient enterprise*: *Overcoming vulnerability for competitive advantage*. MIT Press.

Silvestri, S., Islam, S., Amelin, D., Weiler, G., Papastergiou, S., & Ciampi, M. (2024). Cyber threat assessment and management for securing healthcare ecosystems using natural language processing. *International Journal of Information Security*, *23*, 31–50. https://doi.org/10.1007/s10207-023-00769-w

Singh, A., & Dubey, S. K. (2024, March). Analytical approach towards cybersecurity through AI-enabled threat intelligence. In *2024 11th International Conference on Reliability*, *Infocom Technologies and Optimization* (*Trends and Future Directions*) (*ICRITO*) (pp. 1–6). IEEE. https://doi.org/10.1109/ICRITO61523.2024.10522422

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems* (NIST Special Publication 800-30). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30

Strandberg, K., Rosenstatter, T., Jolak, R., Nowdehi, N., & Olovsson, T. (2021). Resilient shield: Reinforcing the resilience of vehicles against security threats. In *2021 IEEE 93rd Vehicular Technology Conference* (*VTC2021-Spring*) (pp. 1–7). IEEE. https://doi.org/10.1109/VTC2021-Spring51267.2021.9449029

Taleb, N. N. (2012). *Antifragile*: *Things that gain from disorder*. Random House.

Tsuji, D., Fujita, J., Matsumoto, N., Tamura, Y., Doenhoff, J., & Shigemoto, T. (2023). 3-layer modelling method to improve the cyber resilience in industrial control systems. *SICE Journal of Control*, *Measurement*, *and System Integration*, *16*(1), 63–74. https://doi.org/10.1080/18824889.2023.2177074

Umunnakwe, A., Sahu, A., Narimani, M. R., Davis, K., & Zonouz, S. (2021). Cyber-physical component ranking for risk sensitivity analysis using betweenness centrality. *IET Cyber-Physical Systems*: *Theory* & *Applications*, *6*(3), 139–150. https://doi.org/10.1049/cps2.12010

Veeramany, A., Unwin, S. D., Coles, G. A., Dagle, J. E., Millard, D. W., Yao, J., Glantz, C. S., & Gourisetti, S. N. (2016). Framework for modeling high-impact, low-frequency power grid events to support risk-informed decisions. *International Journal of Disaster Risk Reduction*, *18*, 125–137. https://doi.org/10.1016/j.ijdrr.2016.06.008

Virglerova, Z., Panić, M., Voza, D., & Veličković, M. (2021). Model of business risks and their impact on operational performance of SMEs. *Economic Research-Ekonomska Istraživanja*, *35*(1), 4047–4064. https://doi.org/10.1080/1331677X.2021.2010111

Wai, E., & Lee, C. K. M. (2023). Seamless Industry 4.0 integration: A multilayered cyber-security framework for resilient SCADA deployments in CPPS. *Applied Sciences*, *13*(21), Article 12008. https://doi.org/10.3390/app132112008

Yeboah-Ofori, A., & Islam, S. (2019). Cyber security-resilient supply chain network architecture based on cyber threat intelligence. *Computers* & *Security*, *80*, 1–17.

Youssef, S. B. H., & Boudriga, N. (2021). A resilient micro-payment infrastructure: An approach based on blockchain technology. *Kuwait Journal of Science*, *49*(1). https://doi.org/10.48129/kjs.v49i1.10578

Zelle, D., Plappert, C., Rieke, R., Scheuermann, D., & Krauß, C. (2022). ThreatSurf: A method for automated Threat Surface assessment in automotive cybersecurity engineering. *Microprocessors and Microsystems*, *90*, Article 104461. https://doi.org/10.1016/j.micpro.2022.104461