The Balanced Chance & Cyber-Risk Card: Extending Reichmann's Multidimensional Controlling Framework for C-Level Steering in SMEs

Alexander Lawall
IU International University of Applied Sciences
Erfurt, Thüringen, Germany
e-mail: alexander.lawall@iu.org

Maik Drozdzynski
IU International University of Applied Sciences
Erfurt, Thüringen, Germany
e-mail: maik.drozdzynski@iu.org

***Abstract*—Cyber threats pose a growing strategic challenge for German Small and Medium-Sized Enterprises (SMEs), yet existing management control systems offer limited tools to integrate cybersecurity into executive steering. This paper introduces the Balanced Chance & Cyber-Risk Card (BCCR-Card) – an extension of Reichmann's multidimensional controlling framework – designed to embed cyber-specific Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) into a five-dimensional control structure. By aligning operational metrics (e.g., Mean Time To Detect (MTTD), patch latency) with strategic indicators (e.g., Cyber Value at Risk (CyVaR), Expected Annual Loss (EAL)), the BCCR-Card bridges technical cybersecurity telemetry and C-level decision-making. The framework supports role-specific dashboards and maps directly to standards, such as ISO 31000, National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, and Corporate Stabilisation and Restructuring Act (StaRUG) compliance requirements. A tiered KPI logic and scenario-based stress testing ensure traceability and audit readiness. The model transforms cybersecurity from a siloed IT concern into a board-level control dimension, enabling risk-informed leadership and resilience planning. While further empirical validation is needed, the BCCR-Card offers a scalable foundation for integrating cyber risk into enterprise performance management.**

Keywords-Cyber Risk Management; Enterprise Risk Management (ERM); Risk Controlling in SMEs; Management Control Systems; Cybersecurity Metrics; Balanced Scorecard.

I. INTRODUCTION

Over the past decade, the risk landscape for German enterprises has been reshaped by cybercrime. In 2024, the Federal Criminal Police Office recorded 131,391 domestic cybercrime offences – 9% more than in 2023 – and 950 officially reported ransomware incidents [1]. The economic impacts are equally notable: according to Bitkom's Wirtschaftsschutz 2024, cyber-attacks alone (exclusive of other forms of white-collar crime) caused € 178.6 billion in losses on Germany's economy, while eight out of ten firms experienced at least one successful attack within the preceding twelve months [2].

The cyber threats continue to grow. The Federal Office for Information Security (BSI) identified a daily average of 309,000 new malware variants in its 2024 situation report – an increase of 26% year-on-year [3]. These attacks translate directly into balance-sheet risks: IBM's Cost of a Data Breach 2024 puts the mean loss per breach in Germany at USD 5.31 million, up from USD 4.67 million a year earlier [4]. Perceptions inside companies are converging with these figures; the Hiscox Cyber Readiness Report 2024 notes that 67% of surveyed firms faced more attacks than in the prior year and a majority classify their cyber risk exposure as "high" [5].

As a consequence, cybersecurity has moved onto the management agenda of controlling departments. Controlling founder Horváth lists cyber risk management, alongside Environmental, Social and Corporate Governance (ESG) reporting, among the fastest-growing controlling disciplines for CFOs in 2024 [6]. Yet existing research still lacks an integrated steering framework that treats cyber risks on an equal footing with classical corporate-risk categories. The Balanced Chance & Risk Card proposed in 2000 [7] and updated alongside the Law on Control and Transparency in the Corporate Sector (KonTraG) in 2001 [8, pp. 282] by German controlling pioneer Reichmann offers a conceptual anchor as a breakthrough in risk-management, but has so far not been extended with cyber-specific KRIs. Likewise, the risk-controlling process by German leading risk-management researcher Diederichs provides a systemic approach and does not yet incorporate the distinctive dynamics of cyber-threat scenarios [9, pp. 189].

Adding to the urgency, the StaRUG, in force since January 1st, 2021, obliges German SMEs of any legal form to establish an early-warning system for existential risks, implicitly requiring a proportionate risk-controlling architecture [10]. Cyber threats now constitute the most prominent risk class within this mandate, which significantly emphasizes the need to establish a corporate cyber risk integrated controlling framework to guarantee optimized steering capabilities.

This study closes the identified gap by introducing a BCCR-Card – an extension of the Reichmann framework that embeds quantifiable cyber KRIs and aligns them with traditional financial and operational metrics. Building on the classical risk-controlling cycle (identification, assessment, steering, monitoring), we (i) derive a set of cyber-specific steering indicators, (ii) integrate them into the BCR-Card, and (iii) demonstrate applicability through a mid-sized manufacturing case. The result is a practicable concept that enables top management and controllers alike to treat cyber risks as a first-class steering dimension within the regular corporate reporting.

The remainder of the paper is structured as follows. Section II reviews the theoretical foundations of corporate risk management, Reichmann's multidimensional controlling framework, and the Balanced Chance and Risk Card. Section III presents the proposed BCCR-Card as a cyber risk-oriented extension, detailing its dimensions, KPIs/KRIs, and cause-

effect logic. Section IV discusses limitations, implications, and directions for future research. Section VI concludes by summarizing the contributions and positioning the BCCR-Card as a scalable tool for embedding cyber risk into enterprise performance management.

II. Theoretical Foundation

A. Corporate Risk Management

In managerial accounting, risk management refers to the systematic handling of uncertainties that may impair, or enhance, the achievement of corporate objectives [9]. From an expected-value perspective, risk is the dispersion of potential outcomes around a planned value [7]. Hopkin further argues that modern frameworks must recognize the upside of uncertainty and integrate opportunity management into corporate steering [11, p.472].

The legal framework in Germany mandates an enterprise-wide early-warning system:

1) Section 91(2) of the Stock-Corporation Act, enacted through the KonTraG (1998), obliges listed boards to detect developments that could threaten their going concern [12].
2) The StaRUG (effective January 1st, 2021) extends this duty to all limited-liability entities by requiring "continuous crisis detection" [10].

However, the key challenge remains that, although the StaRUG formally requires early-crisis detection, even for small private limited companies (GmbHs), enforcement still operates through civil and insolvency liability rather than administrative penalties. Accordingly, a GmbH that fails to establish such a system exposes itself to potential civil or insolvency claims and may incur less favourable insurance terms or downgraded ratings from banks and rating agencies.

The international guidelines refine the process. ISO 31000:2018 embeds risk management within governance structures, while Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management (COSO ERM) 2017 operationalises a four-step cycle of (i) Identify, (ii) Assess, (iii) Respond, and (iv) Monitor [13].

Following this tradition, Diederichs draws a clear line between risk management (strategic orientation) and risk controlling (information supply and steering). Risk controlling comprises (i) quantitative appraisal through scenario and sensitivity analyses, (ii) portfolio aggregation into metrics, such as Value at Risk, and (iii) stakeholder-specific reporting to boards and operational units [9].

This paper adopts this canonical four-phase model as its methodological basis, but focuses on a critical gap: digital threat scenarios. Recent German threat reports show high malware volumes and escalating breach costs. Traditional taxonomies must be expanded to encompass cyber risks, ensuring compliance with statutory requirements and alignment with evolving technological realities.

B. Multidimensional Controlling Concept by Reichmann

The multidimensional controlling concept developed by Thomas Reichmann is considered a reference model in German-language management control, because it integrates functional responsibilities, information logic, and time horizons within a single, coherent framework [14, pp. 21]. At its core, controlling is defined as an IT-supported, decision-oriented management service: every decision-maker should receive exactly the information that matches their task, planning horizon, and area of responsibility.

The model is built around a data cube with three orthogonal dimensions. (i) Functional view (e.g., cost- and profit-, financial, or procurement controlling) allocates information along the value chain and thus provides an impact-oriented perspective. (ii) Information categories separate monetary profit- and cash-flow figures from operational quantity and quality data, enabling quantitative metrics to be combined with qualitative early-warning indicators. (iii) Time horizons distinguish strategic, tactical, and operational scopes; consequently, short-term variance analyses and long-term trend observations can coexist within the same data model.

Reichmann links the cube to a three-level information pyramid to keep the data volume manageable [14, pp. 13]. On the accounting layer, raw booking and voucher data are captured. The reporting layer aggregates these into management reports featuring plan/actual comparisons. At the top, the key-figure layer compresses the data further into leading and structural ratios, among them the RL ratio system designed by Reichmann and Lachnit [14, p. 87], which provides rapid steering impulses. Data flow is strictly bottom-up for aggregation and top-down for target values, ensuring consistency between operational detail and strategic metrics.

The concept is practically relevant due to its integration blueprint, where each dimension assumes a distinct role in the IT architecture. Fact and dimension tables in a data warehouse map functions, information categories, and time horizons. Extract, Transformation and Load (ETL)-processes transport booking data up to the key-figure layer and dashboards. Planning, actual, and forecast values can therefore be compared across all levels without media or aggregation breaks. In practice, boards decide based on top-level KPIs (Return on Investment, working-capital ratio, etc.), while divisional managers drill down to variance reports. Meanwhile, operational controllers still work with itemized lists.

Finally, the concept supports early-warning and scenario analyses: qualitative indicators (e.g., Threats or market-trend signals) are stored as a distinct information category and can be combined with monetary KPIs. Organisations thus detect opportunities and risks earlier and can simulate response options before effects appear in the income statement.

In summary, Reichmann's multidimensional concept provides a robust bridge between a company's goal system and its technical implementation, allowing for traceable aggregation from primary data to key figures and providing role-specific access to the exact level of information granularity required

for sound management decisions.

Reichmann's merit lies not only in having proposed a controlling framework in the mid-1980s, but also in designing it to stay compatible with future technologies and thus continuously extensible. Although conceived decades ago, the model is regularly adapted to new industries and technologies, allowing emerging controlling sub-disciplines, such as risk management, to be integrated without altering its core. For example, Drozdzynski embeds medical performance data and BI dashboards into the system- and application-layers of Reichmann's cube for a hospital context [15], while Liebe and Drozdzynski extend the framework to health-and-social-care organisations [16]. These adaptations demonstrate that the cube's general part remains comparable across sectors, whereas its special part can be customised with domain-specific metrics.

C. Balanced Chance & Risk Card

The Balanced Chance and Risk Card (BCRC) was introduced by Reichmann as an extension of the Balanced Scorecard (BSC) to meet the tighter German regulatory requirements for integrated risk management, such as KonTraG, at the beginning of the 2000s [17] [8]. Diederichs subsequently operationalised the concept for controlling practice and anchored it in the German "Controlling" journal [18]. The instrument combines value-based management, the BSC logic, and systematic opportunity-and-risk control within a single reporting artefact.

Several authors recommend a six-step implementation procedure: (i) define strategic goals per perspective, (ii) derive appropriate performance KPIs, (iii) identify and evaluate the main opportunities and risks (probability $\times$ impact), (iv) link KPIs with the respective opportunities/risks to obtain risk-adjusted targets and actuals, (v) specify measures, owners and milestones, and (vi) install a rolling review cycle (monthly or quarterly). This procedure merges strategy progress, risk exposure, and action effectiveness into a single management view.

While the BCRC is conceived as an entirely risk-oriented steering framework, recent applications mention cyber threats only in passing as a subset of generic operational risks and provide neither dedicated KRIs nor tailored control routines for them [18]. Considering the accelerating frequency, networked propagation and potentially existential financial impact of contemporary cyber incidents, it is timely and methodologically warranted to give cybersecurity risks disproportionate analytical weight within the BCRC [19]. Section II-D therefore examines the nature and managerial relevance of cybersecurity risks as a prerequisite for their systematic integration into the card.

D. Cybercrime & Cybersecurity

Recent research highlights the importance of integrating real-time Cyber Threat Intelligence (CTI) into dynamic risk management systems to enable situational awareness [20]. A semantic web technology-based architecture is introduced to create a dynamic risk assessment system at operational, tactical, and strategic levels [21]. A further development is the concept with an ontology-driven real-time risk management approach that encompasses anomaly detection and cataloging vulnerabilities [22]. The requirement for automated technologies to offer situational awareness solutions for National Cyber Operation Centers is pointed out by [23]. An example in practice suggests a Metrics Visualization System that can dynamically visualize network security incidents and correlate them with risk levels [24]. Collectively, these studies emphasize the potential for real-time, standardized operational cyber threat metrics to enhance decision-making across hierarchy levels, from administrators to the C-suite, through a more timely and accurate assessment of an organization's cybersecurity position.

CTI has proved to be an essential way of supplementing cybersecurity and risk management in organizations. CTI significantly increases threat detection, response, and risk management capability [25]. CTI provides evidence-based insight into the threats to facilitate proactive risk mitigation in critical infrastructure [26]. CTI can be integrated into campaigns for raising awareness against cyberattacks, especially in the banking sector, through the use of tactical, operational, and strategic intelligence [27] [20]. In response to the need for real-time risk analysis, a semantic-based architecture using Web Ontology Language (OWL) and Semantic Web Rule Language (SWRL) has been proposed, such as Structured Threat Information eXpression (STIX) v2.0 for the structured exchange of threat information [21]. Despite its advantages, there are barriers to CTI adoption, including technological constraints and the absence of executive sponsorship. These issues need to be overcome through extensive awareness programs, executive participation, and systematic training efforts [25].

III. A Cyber Risk-Oriented Extension of the Reichmann Framework

A. Limitations of Classical Risk Assessment Models in Cyber Contexts

Classical risk-assessment frameworks have challenges in cyber domains for four core reasons. First, scarce loss data leave actuarial or scenario models without reliable frequency and severity inputs citeElingSchnell2022. Second, traffic-light heat maps compress complex threats into ordinal colours, masking value at stake and skewing priorities [28]. Third, adversarial tactics evolve weekly, so annual risk registers are inappropriate, as European Union Agency for Cybersecurity (ENISA) 2024 survey warns [29]. Fourth, cloud and supply-chain interdependence creates cascade-prone losses; single-asset Value at Risk (VaR) thus understates extremes [30]. Embedding cyber KRIs in Reichmann's multidimensional controlling framework, especially into the BCR-Card, ties exposure to profitability-liquidity goals and helps close these gaps.

B. A Structured Controlling Concept for Cyber Metrics

Modern organisations face data overload and goal conflicts. An integrated controlling concept mitigates both by

(i) aligning metrics with strategic objectives, (ii) enforcing a common language for financial and non-financial data, and (iii) enabling transparent, audit-ready decision trails [31, pp. 7] [32, pp. 5]. Research shows that companies with coherent management-control systems achieve higher decision quality and risk resilience than those using ad-hoc indicator sets [33, pp. 30].

Applying this logic to cybersecurity avoids metric issues: isolated dashboards might track patch rates or incident counts, yet without linkage to profitability and liquidity, they lack managerial traction. Embedding cyber-risk KPIs into Reichmann's cube – e.g., as an additional information category on the system layer – ensures goal congruence (security spend vs. value at risk), comparability (cross-unit benchmarking), and governance compliance (StaRUG early-warning duties). Hence, a structured concept is not academic ornamentation but a prerequisite for turning raw cyber data into actionable, strategy-consistent steering information.

The proposed framework introduces cyber resilience as a fifth dimension besides the well-known four dimensions: finance, growth, internal processes, and customer/market. Clear roles and responsibilities ensure accountability, like the Chief Executive Officer (CEO)/ Chief Financial Officer(CFO) owns capital allocation and is in charge of gaining profitability and driving financial return. The top management, e.g., Vice President Sales (VPS), owns the Market/Customer perspective. The Chief Information Security Officer (CISO) operates the technical control loop and supplies metrics alongside the perspective *cyber resilience*. The following concept will not discuss the steering capabilities of the balanced scorecard in general, but will focus on the steering levers in the field of cyber risk management.

C. Extension Modules for the Cyber Risk-Oriented BCRC

Building on the original BCRC, five enhancements build a foundation in the context of handling cyber risks:

1) Add a dedicated **Cyber Resilience** perspective. This fifth view elevates cyber threats to the same strategic level as Finance, Customer, Process and Learning, following the Balanced Scorecard logic already adopted by security leaders.
2) Embed **cyber-specific KRIs** into every perspective. Examples include CyVaR under Finance, Customer-trust indices under Customer/Market, Mean Time to Patch for Processes, and secure-coding coverage in Learning.
3) **Cross-walk** each KRI to NIST Cybersecurity Framework (CSF 2.0). Mapping metrics to the Identify-Protect-Detect-Respond-Recover-Govern functions provides audit-ready consistency and international comparability.
4) Introduce a **scenario- and stress-test layer**. A cyber scenario sheet quantifies best-likely-worst losses and mirrors the board-level logic of a cyber-risk balance sheet.
5) Apply **dynamic weighting and alerting**. Weekly (or faster) refreshes of KRI scores from Security Operations Center (SOC) telemetry, threat intelligence feeds, and vulnerability scanners keep the BCRC heat-map aligned with the shifting threat landscape.

D. KPIs in Cybersecurity

A tiered KPI system is essential, aligning *strategic KPIs* for top management with *operational metrics* for CISOs, middle management, and IT administrators to effectively integrate cybersecurity into corporate steering, particularly in SMEs.

Strategic KPIs, such as the CyVaR, Expected Annual Loss, or a Cyber Resilience Index, translate technical risks into financial terms [34] [8]. These figures support board-level steering decisions and ensure compliance with regulatory duties, such as those mandated by the StaRUG, which requires continuous monitoring of existential threats [10].

Operational KPIs, including (MTTD), Mean Time to Respond (MTTR), and Patch Compliance Rate, measure the effectiveness of technical controls. A decreasing MTTD, for example, indicates faster breach detection, while increasing patch compliance reflects reduced vulnerability exposure [28] [35]. These indicators, typically monitored via SOC dashboards, inform tactical actions and feed into higher-level summaries.

A *role-specific allocation* of KPIs ensures managerial relevance: while C-levels need aggregated dashboards on residual risk, CISOs interpret trends in departmental exposure, and SOC staff focus on technical telemetry. Reichmann's multi-dimensional controlling model supports this by aggregating data bottom-up while cascading targets top-down [14].

KPIs should map onto international standards to ensure auditability and governance alignment. The NIST CSF 2.0 recommends outcome-based metrics across its core functions (Identify, Protect, Detect, Respond, Recover, Govern) [36] [37], while ISO/IEC 27001 and ISO/IEC 27004 call for structured monitoring and evaluation of Information Security Management System (ISMS) performance [38]. Mapping MTTD to "Detect" or patch compliance to "Protect" enhances traceability and facilitates compliance checks.

We propose a practical KPI pyramid logic:

1) **Strategic layer (CEO/CFO):** e.g., CyVaR, residual cyber risk index, compliance readiness.
2) **Tactical layer (CISO/Chief Information Officer (CIO):** e.g., maturity scores, awareness coverage, open vulnerabilities.
3) **Operational layer (SOC/Admin):** e.g., phishing susceptibility, patch latency, intrusion attempts.

At the base, CTI provides real-time data (e.g., vulnerability alerts, attack vector trends) [25] [21]. These are aggregated into composite indicators, such as a Threat Intelligence Index, which informs middle and upper management of current threat exposure and supports adaptive countermeasures.

Furthermore, distinguishing between *gross (inherent)* and *residual (net)* cyber risk is essential. This enables management to assess the effectiveness of existing controls. For example, if the inherent ransomware risk is high, but the residual risk is low due to segmentation and offline backups, no immediate investment is needed. German legal standards under

KonTraG and StaRUG explicitly require this level of risk quantification [12] [10].

In summary, embedding cyber KPIs into a multidimensional controlling system bridges technical telemetry and strategic steering. For SMEs, this approach is not only methodologically sound but regulatory-aligned, promoting a risk-aware leadership culture with measurable security accountability.

E. The Balanced Chance & Cyber Risk Card

Table I translates Reichmann's multidimensional framework into a five-perspective dashboard that makes cyber risks "board-ready". Each perspective shows *value drivers* (KPI) and *residual-risk indicator* (KRI). The Finance row anchors the card with the Return on Capital Employed (ROCE) [14, p. 131] and the ratio EAL/Earnings Before Interest and Taxes (EBIT), while *CyVaR95%-intensity* expresses cyber exposure to the revenue [39]. Market & Customer links digital availability to loyalty by pairing the Net-Promoter-Score with service downtime. Internal Processes connects OEE to vulnerability management. Learning & Growth captures the human attack surface; and the dedicated Cyber-Resilience view merges technical readiness (MTTR, MTTD) with an aggregate Cyber-Resilience-Index [29]. Horizons (strategic, tactical, operational) follow Reichmann's time axis, ensuring that indicators are reported at the level where they can be acted upon.

All KPIs/KRIs should use a three-step traffic-light logic. The limits depend on the branch and the individual business, but as a rule of thumbs, one can firstly go with the following suggestion:

- **Green:** on or better than target;
- **Yellow:** target–10% (warning);
- **Red:** $\geq$ 10% deviation, triggering an escalation to the next management tier and a liquidity stress-test in line with StaRUG early-warning duties.

F. Illustrative Cause–Effect Chains

Chain 1: Patch backlog $\rightarrow$ Production efficiency $\rightarrow$ Financial impact: A rising patch latency (Red at $>$14 days) increases exploit probability; the resulting micro-outages degrade OEE. Each OEE point lost raises unit cost by 0.4%, reducing ROCE and lifting CyVaR95%. If CyVaR passes the 5%-of-revenue threshold, the Finance cell flips to Yellow, prompting additional patch sprints and a review of the cyber-insurance cap.

Chain 2: Phishing awareness $\rightarrow$ Incident detection $\rightarrow$ Resilience: Quarterly awareness training pushes the phishing click-rate below 5% (Green). MTTD for phishing drops from 48h to 12h, which, with unchanged MTTR, cuts the Cyber Resilience Index gap by 7 points. When the index exceeds the 80-point target, the Resilience perspective turns Green, signalling sufficient buffer to keep CyVaR and EAL/EBIT within Finance targets.

These chains demonstrate how the BCCR-Card connects technical metrics to profitability and liquidity, enabling top management to prioritise cyber investments on a value-at-risk basis while satisfying the integrative control logic advocated by Reichmann.

IV. Discussion and Outlook

The BCCR-Card integrates cyber exposure to Reichmann's profitability–liquidity logic, yet several reservations remain. First, the proposal models frequencies and loss-severities; data scarcity and under-reporting continue to limit the statistical confidence of CyVaR and EAL estimates [39]. Second, the traffic-light logic simplifies dynamic attack surfaces into discrete states; abrupt threshold effects may hide early trend deterioration. Third, transferring the card across industries requires recalibrating KPIs/KRIs, e.g., patch latency is less relevant for cloud-natives than for Operational Technology (OT) environments, which challenges cross-company benchmarking.

Future research should focus on four components: (i) *Empirical validation*: multi-case studies that track KPI/KRI trajectories over 12-18 months could test whether red-or-yellow signals indeed precede financial variance. (ii) *Automated data feeds*: integrating Security Information and Event Management (SIEM) and Enterprise Resource Planning (ERP) streams via Application Programming Interfaces (APIs) will reveal how latency and data-quality issues distort CRI and CyVaR. (iii) *Artificial Intelligence (AI)-driven scenario generation*: Large Language Models could widen the threat catalogue beyond historical events and improve tail-risk estimation. (iv) *ESG-Cyber overlaps*: regulators increasingly frame cybersecurity as a governance pillar; embedding ESG metrics into the BCCR-Card would extend its relevance for integrated reporting. Addressing these gaps will raise the explanatory power of the card and help verify whether the hypothesised cause–and–effect chains hold across organisational contexts [33] [29].

V. SME Adoption, Generalizability, and Lessons Learned

This section offers a concise methodology for SMEs, discusses generalizability beyond the German context, and summarizes lessons learned alongside future technical work from applying the BCCR-Card.

A. Methodology for SME Adoption

Effective use of the BCCR-Card starts with clear ownership and cadence at C-level, typically shared between finance and security leadership (e.g., CFO and CISO), with a monthly review focused on decisions rather than dashboards. Organizations select a small set of indicators. Ideally, no more than two per perspective to preserve attention on what moves value and resilience. Each indicator is defined in one sentence (scope, unit, and aggregation), assigned a single quarterly target, and governed by stable green/yellow/red thresholds to allow trend interpretation. A minimal measurement layer reuses existing sources such as ticketing, endpoint management, SIEM, and backup reports, complemented by plausibility checks and

TABLE I
THE BALANCED CHANCE & CYBER RISK CARD

Perspective	Responsability	Horizon	KPI/KRI	Target
Finance	CEO / CFO	strategic $>$ 3 *Years*	ROCE CyVaR95%-intensity EAL / EBIT	ROCE $\geq$ 10% CyVaR95 $\leq$ 5% EAL / EBIT $\leq$ 10%
Market & Customer	Top Management	strategic-tactical *1-3 Years*	Net Promoter Score (NPS) Service downtime per customer (in min/yr)	NPS $\geq$ 60 Downtime $\leq$ 30 min
Internal Processes	Middle Management	tactical-operational *Quarter-1 Year*	Overall Equipment Effectiveness (OEE) Patch latency of critical systems (in days) Patch-Compliance-Rate (PCR)	OEE $\geq$ 85% Latency $\leq$ 14d PCR $\geq$ 95%
Learning & Growth	Team Level	operational *month-year*	Training hours per employee and year Phishing click-through rate (in %)	$\geq$ 24h $\leq$ 5%
Cyber Resilience	CISO & IT ops	operational-strategic *Day-Year*	Cyber Resilience Index (CRI) MTTR MTTD Backup-restore success rate (in %)	$\geq$ 80% MTTR $\leq$ 2h MTTD $\leq$ 24h $\geq$ 98%

temporary proxies where data coverage is incomplete. Two tabletop scenarios (e.g., ransomware and supplier outage) are used to translate operational signals into financial exposure via EAL and CyVaR. Approved actions are tracked against loss reduction and expenses, with quarterly reporting of EAL/EBIT and the ROCE of controls. In practice, SMEs can achieve a viable first loop within 90 days by fixing ownership and thresholds, assembling a single-page card with the most accessible data, running two scenarios, and replacing estimates with measured values as coverage improves.

B. Generalizability

While our examples reference German regulation, the design itself widely adopted frameworks (NIST CSF and ISO/IEC 27001) and governance principles compatible with COSO ERM. Sector characteristics primarily affect indicator choice (e.g., they choose the KPI liquidity ratio instead of ROCE) and data availability. The cause–and–effect logic and the financial coupling through EAL and CyVaR remain invariant. Very small companies can reduce scope to a single value stream without undermining the control logic.

C. Lessons Learned and Challenges

Across pilots, too many indicators weaken focus, frequent threshold changes flasify trends, and incomplete telemetry invites false precision if point estimates are reported without ranges. Persistently red signals require explicit decision mapping, a quick fix, structural control, or risk acceptance, to avoid loss. Finally, finance and security communities use different vocabularies. The BCCR-Card works as a shared language when explanations stay close to economics and risk awareness.

VI. CONCLUSION AND FUTURE WORK

This study presents the Balanced Chance & Cyber-Risk Card as a novel extension of Reichmann's multidimensional controlling framework, addressing a critical gap in cyber risk integration for German SMEs. By embedding cyber-specific Key Risk Indicators and Key Performance Indicators into a five-dimensional control structure, the model enables a seamless translation of technical security telemetry into strategic, tactical, and operational steering metrics. The framework aligns with regulatory imperatives, such as StaRUG, ISO 31000, and NIST CSF 2.0, ensuring compliance-readiness while enhancing auditability and executive decision-making.

Through role-specific dashboards, cause–effect chains, and scenario-based stress testing, the BCCR-Card enables the C-suite to quantify cyber resilience and align investments with value-at-risk priorities. It makes cybersecurity a core component of enterprise performance management. The framework offers a basis for empirical validation, AI-driven scenarios, and ESG integration. Ultimately, the BCCR-Card embeds cyber risk into measurable, board-level control-bridging financial steering with digital threat management.

REFERENCES

[1] Bundeskriminalamt, "Bundeslagebild Cybercrime 2024 [Federal Situation Report Cybercrime 2024]," Bundeskriminalamt, Wiesbaden, Germany, Tech. Rep., Jun. 2025, [retrieved: July, 2025]. [Online]. Available: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2024/CC_2024.html

[2] Bitkom e. V., "Wirtschaftsschutz 2024 - Cybercrime in der deutschen Wirtschaft [Economic Protection 2024 - Cybercrime in the German Economy]," Bitkom e. V., Berlin, Germany, Tech. Rep., Aug. 2024, [retrieved: July, 2025]. [Online]. Available: https://www.bitkom.org/Presse/Presseinformation/Angriffe-auf-die-deutsche-Wirtschaft-nehmen-zu

[3] Bundesamt für Sicherheit in der Informationstechnik, "Die Lage der IT-Sicherheit in Deutschland 2024 [The State of IT Security in Germany 2024]," Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany, Tech. Rep., Nov. 2024, [retrieved: July, 2025]. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html?nn=129410

[4] IBM Security, "Cost of a Data Breach Report 2024," IBM Security, Armonk, NY, USA, Tech. Rep., 2024, [retrieved: July, 2025]. [Online]. Available: https://www.ibm.com/reports/data-breach

[5] Hiscox, "Cyber Readiness Report 2024," Hiscox Ltd., London, U.K., Tech. Rep., 2024, [retrieved: July, 2025]. [Online]. Available: https://hiscoxdedrupal.prod.acquia-sites.com/sites/default/files/documents/hiscox-cyber-readiness-report-2024.pdf

[6] Horváth & Partners Management Consultants, "CFO Study 2024: The CFO's Path to a data Driven Company," Horváth & Partners, Stuttgart, Tech. Rep., Jul. 2024, [retrieved: July, 2025].

[Online]. Available: https://www.horvath-partners.com/en/media-center/studies/cfo-study-2024-the-cfos-path-to-a-data-driven-company

[7] T. Reichmann and S. Form, "Balanced Chance- and Risk-Management," *Controlling – Zeitschrift für erfolgsorientierte Unternehmenssteuerung*, vol. 12, no. 4/5, pp. 189–198, 2000.

[8] T. Reichmann, "Die Balanced Chance- and Risk-Card: Eine Erweiterung der Balanced Scorecard [The Balanced Chance and Risk Card: An Extension of the Balanced Scorecard]," in *Risikomanagement nach dem KonTraG – Aufgaben und Chancen aus betriebswirtschaftlicher und juristischer Sicht*, K. W. Lange and F. Wall, Eds. München: Franz Vahlen, 2001, pp. 282–303.

[9] M. Diederichs, *Risikomanagement und Risikocontrolling [Risk Management and Risk Controlling]*, 5th ed. München: Franz Vahlen, 2023.

[10] Bundesrepublik Deutschland, "Gesetz über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen (Unternehmensstabilisierungs- und -restrukturierungsgesetz – StaRUG) [Law on the Stabilization and Restructuring Framework for Companies (Corporate Stabilization and Restructuring Act – StaRUG)]," Bundesgesetzblatt I, Nr. 66, 29. Dez. 2020, S. 3256–3340, Dec. 2020, [retrieved: July, 2025]. [Online]. Available: https://www.gesetze-im-internet.de/starug/BJNR325610020.html

[11] P. Hopkin and C. Thompson, *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Enterprise Risk Management*, 6th ed. London: Kogan Page, 2022.

[12] Bundesrepublik Deutschland, "Aktiengesetz (AktG) [Stock Corporation Act]," Bundesgesetzblatt I 1965, S. 1089; zuletzt geändert durch Art. 1 Gesetz vom 21. Dez. 2023, BGBl. I 2023 Nr. 394, Sep. 1965, [retrieved: July, 2025]. [Online]. Available: https://www.gesetze-im-internet.de/aktg/BJNR010890965.html

[13] *Risk Management-Guidelines (ISO 31000:2018)*, International Organization for Standardization Std., Feb. 2018.

[14] T. Reichmann, M. Kißler, and U. Baumöl, *Controlling mit Kennzahlen: Die systemgestützte Controlling-Konzeption [Controlling with Key Figures: The System-Supported Controlling Concept]*, 9th ed. München: Franz Vahlen, 2017.

[15] M. Drozdzynski, *Das neue Business Intelligence-gestuetze Krankenhaus-Controlling [The New Business Intelligence-Supported Hospital Controlling]*. Baden-Baden: Nomos, 2020.

[16] M. Liebe and M. Drozdzynski, "IT-gestützte Ausgestaltung einer GeSo-spezifischen mehrdimensionalen Controlling-Konzeption [IT-Supported Design of a Health and Social Care-Specific Multidimensional Controlling Concept]," *Controlling – Zeitschrift für erfolgsorientierte Unternehmenssteuerung*, vol. 30, no. 4, pp. 31–40, 2018.

[17] R. S. Kaplan and D. P. Norton, "The Balanced Scorecard – Measures That Drive Performance," *Harvard Business Review*, vol. 70, no. 1, pp. 71–79, 1992.

[18] M. Diederichs, "Balanced Chance- & Risk-Card," *Controlling*, vol. 16, no. 12, pp. 703–705, 2004.

[19] ISACA. (2024, Apr.) How CISOs Can Take Advantage of the Balanced Scorecard Method. [retrieved: July, 2025]. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2024/how-cisos-can-take-advantage-of-the-balanced-scorecard-method

[20] A. Lawall and P. Beenken, "A Threat-Led Approach to Mitigating Ransomware Attacks: Insights from a Comprehensive Analysis of the Ransomware Ecosystem," in *Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference*, ser. EICC '24, S. Li, K. Coopamootoo, and M. Sirivianos, Eds. New York, NY, USA: Association for Computing Machinery, 2024, pp. 210–216. [Online]. Available: https://doi.org/10.1145/3655693.3661321

[21] R. Riesco and V. A. Villagrá, "Leveraging cyber threat intelligence for a dynamic risk framework: Automation by using a semantic reasoner and a new combination of standards (stix™, swrl and owl)," *International Journal of Information Security*, vol. 18, no. 6, pp. 715–739, 2019.

[22] C. Sánchez-Zas, V. A. Villagrá, M. Vega-Barbas, X. Larriva-Novo, J. I. Moreno, and J. Berrocal, "Ontology-based approach to real-time risk management and cyber-situational awareness," *Future Generation Computer Systems*, vol. 141, pp. 462–472, 2023.

[23] R. Graf, F. Skopik, and K. Whitebloom, "A decision support model for situational awareness in national cyber operations centers," in *2016 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*. IEEE, 2016, pp. 1–6.

[24] T. Väisänen, S. Noponen, O.-M. Latvala, and J. Kuusijärvi, "Combining real-time risk visualization and anomaly detection," in *Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings*, 2018, pp. 1–7.

[25] J. Smallman, "The effectiveness of cyber threat intelligence in improving security operations," *Journal of Artificial Intelligence General science (JAIGS) ISSN:3006-4023*, vol. 5, no. 1, p. 189–209, Jul. 2024. [Online]. Available: https://ojs.boulibrary.com/index.php/JAIGS/article/view/193

[26] H. Kure and S. Islam, "Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure," *Journal of Universal Computer Science*, vol. 25, no. 11, pp. 1478–1502, 2019.

[27] R. A. Firdaus, N. A. Rakhmawati, and F. Samopa, "A state-of-the-art review of cyber threat intelligence awareness programs in mitigating bank cyber attacks," in *2024 IEEE International Symposium on Consumer Technology (ISCT)*. IEEE, 2024, pp. 648–654.

[28] S. Myerson, "Why Heat Maps Fail for Cybersecurity Risk Management," Gartner, Inc., Research Note G00734212, September 2023.

[29] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2024," Athens, Tech. Rep., 2024, [retrieved: July, 2025]. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[30] M. Eling, U. Kühn, and H. Gruber, "Modelling Systemic Cyber Risk: Accumulation and Cascade Effects in Interconnected IT Ecosystems," *Journal of Risk Finance*, vol. 24, no. 1, pp. 1–26, 2023.

[31] R. N. Anthony and V. Govindarajan, *Management Control Systems*, 13th ed. New York: McGraw-Hill Education, 2017.

[32] R. Simons, *Levers of Control: How Managers Use Innovative Control Systems to Drive Strategic Renewal*. Boston: Harvard Business School Press, 1995.

[33] K. A. Merchant and W. A. V. der Stede, *Management Control Systems: Performance Measurement, Evaluation and Incentives*, 5th ed. Harlow: Pearson, 2021.

[34] A. Orlando, "Cyber risk quantification: Investigating the role of cyber value at risk," *Risks*, vol. 9, no. 10, p. 184, 2021.

[35] D. S. D. White, "Limiting vulnerability exposure through effective patch management: threat mitigation through vulnerability remediation," Ph.D. dissertation, Rhodes University, 2006.

[36] J. Edwards, *A comprehensive guide to the NIST cybersecurity framework 2.0: Strategies, implementation, and best practice*. John Wiley & Sons, 2024.

[37] "NIST Cybersecurity Framework 2.0 (Draft)," 2024, [retrieved: July, 2025]. [Online]. Available: https://www.nist.gov/cyberframework

[38] "ISO/IEC 27004: Information security management – Monitoring, measurement, analysis and evaluation," [retrieved: July, 2025]. [Online]. Available: https://www.iso.org/standard/73906.html

[39] M. Eling and W. Schnell, "Ten Key Questions for Cyber Risk Modelling: A Systematic Review and Research Agenda," *The Geneva Papers on Risk and Insurance-Issues and Practice*, vol. 47, no. 3, pp. 366–401, 2022.