Bhutan Journal of Business and Management
Published by Gedu College of Business Studies, Royal University of Bhutan
Vol. 9 No. 1 (2026) | https://doi.org/10.17102/bjbm.v9.2

DIAMOND OPEN ACCESS

Cybersecurity Risks and Financial Reporting Integrity amid Digital Transformation in Bhutan

Pema Wangchuk

Jigme Namgyel Engineering College, Royal University of Bhutan, 42002, Dewathang, Samdrup Jongkhar, Bhutan

ABSTRACT

Bhutan's financial system has advanced into the digital space, driven by Digital Drukyul, a significant national information and communication technology (ICT) transformation flagship programme, fostering the use of more ICT to make Bhutan a more digitally connected, smart, and inclusive society. However, such a transformation comes at a cost, and it puts real strain on the integrity of financial reporting, from how assets are valued to whether traditional accounting standards are maintained. This review argues that cyber risk should not be regarded as just an IT-related issue reported in the system. Instead, it builds a framework that integrates digital security breaches directly into the vulnerability of financial statements in an emerging economy of the country. In line with Bhutan's own regulatory and international accounting standards, the study examines seven core accounting areas: (a) how assets and liabilities are valued; (b) how losses are measured; (c) how well internal mechanism controls hold up; (d) how insurance coverage is recognised; (e) whether disclosures are adequate; (f) ensuring regulatory compliance; and (g) how well going concern is assessed. By linking Normative Accounting Theories, Agency, and Stakeholder, the analysis indicates that disconnected ledger systems and relationship-based banking create risk that can shirk cyber-related operational costs and paint a distorted picture of a bank's finances. This study offers a phased, prioritised roadmap for bank leaders, policymakers, and auditors, addressing the gap between digital ambition and fiscal stability as well as aligning stronger resilience with a current digital transformation approach.

Research Article

ARTICLE HISTORY
Received 05-12-2025
Revised 09-06-2026
Accepted 17-07-2026
Published 07-10-2026

KEYWORDS
Cybersecurity, Financial Reporting, Bhutan Accounting Standards, Internal Controls, Disclosure, Regulatory Compliance, AASBB

CORRESPONDING AUTHOR
Pema Wangchuk
pemawangchuk.jnec@rub.edu.bt

DOI
https://doi.org/10.17102/bjbm.v9.2

JOURNAL ISSN
2079-7680 / 2663-1784

Check for article updates

1. Introduction

Globally, the financial landscape is enduring a profound digital transformation, a shift that is nowhere more visible than in the Himalayan Kingdom of Bhutan. Digital Drukyul, a nation's visionary project, is a framework that guides the country's financial sector and supports the move

Citation
Wangchuk, P. (2026). Cybersecurity risks and financial reporting integrity amid digital transformation in Bhutan. *Bhutan Journal of Business and Management*, 9(1), 25-44. https://doi.org/10.17102/bjbm.v9.2

© 2026 The Author(s). Published by Gedu College of Business Studies, Royal University of Bhutan. Authors retain copyright and grant BJBM a non-exclusive publishing right. This Diamond Open Access article is licensed under CC BY 4.0 (creativecommons.org/licenses/by/4.0/), permitting sharing and adaptation with appropriate credit, a licence link, and indication of changes. Authors may share or deposit the published work provided BJBM is acknowledged as the original place of publication and the DOI or formal citation is included.

more quickly to adopt digital directives in pursuit of greater efficiency and inclusion (Royal Monetary Authority of Bhutan [RMA], 2023). Notwithstanding the benefits of this acceleration, it carries a relatively underexamined consequence by increasingly widening the cyber threat surface, including financial institutions exposed to data breaches, system-wide financial fraud, and ransomware. The magnitude of such incidents blows well beyond operational disruption, striking at the fundamentals of financial reporting principles, which include: transparency, verifiability, and faithful representation (Kareem Alsakini, Alawawdeh, & Alsayyed, 2024).

In the international literature review, there is well-established evidence showing the connection between accounting and cybersecurity. In particular, its effects on asset impairment, loss recognition, and financial disclosure practices have more associations (Cremer et al., 2022; Li, No, & Wang, 2018; Singh, 2025).

However, until now, what remains unexplored in the above field are the implications for emerging, inclusive, and digitally aspiring economies such as Bhutan. The country's distinctive regulatory landscape, socio-economic characteristics, and relatively small financial sector create a strong need for research that is grounded in the specific local context rather than relying primarily on frameworks developed elsewhere. To address this gap, the present review pursues three clearly defined objectives, as outlined below:

1. Analyse the material accounting and financial reporting challenges generated by cybersecurity breaches within the financial sector.
2. Contrast international accounting frameworks with Bhutan's current regulatory parameters, such as the RMA guidelines and Bhutan Accounting Standards (BAS), using established theoretical lenses.
3. Formulate a prioritised, academic roadmap for Bhutanese regulators, financial institutions, and academic bodies to mitigate accounting vulnerabilities caused by digital transformation.

This review suggests an integrated framework that links digital risk to the integrity of financial statements and provides evidence-based guidance for central bank regulators and standard-setters through an examination of how cybersecurity breaches reshape accounting and reporting practices in Bhutan.

2. Research Gap

Globally, despite the relationship between financial reporting and cybersecurity risks having gained growing attention among scholars, this systematic review identifies notable thematic and geographical gaps in the existing literature. Moreover, to the author's knowledge, the research carried out for this review returned no eligible studies that specifically examine cybersecurity-related financial reporting or specialised accounting discourses in Bhutan. At the moment, most literature addresses only IT-related operational frameworks, cybersecurity infrastructure, perimeter defence mechanisms, and broader digital transformation initiatives. Conversely, the accounting implications of cybersecurity incidents have not been paid much scholarly attention; far less attention has been paid to the main consequences of the accounting disclosures, transparency, reporting integrity, prudence, and reliability of financial information. This indicates a gap which underscores the need for additional research and investigation by academic scholars into where financial reporting and cybersecurity risks connect and interact within the Bhutanese context for understanding the importance of incidents.

The previous studies on developing nations have examined how international standards, including International Financial Reporting Standards (IFRS) and U.S. Securities and Exchange Commission (SEC)-based frameworks, are implemented across a range of emerging market settings with varying attention to individual nations' specific regulatory and institutional conditions.

However, in Bhutan, the financial sector operates within an institutional and regulatory environment that is moderately concentrated and still emerging with the advancement of new technologies. As reported by the RMA (2023), the credit market was largely concentrated among five commercial banks and three non-banking financial institutions, with 59.9% of the banking sector's loan portfolio managed by the two largest commercial banks. Further, it also reports that the regulatory framework continued to develop in response to emerging digital and financial risks (RMA, 2023). Yet the report highlights only limited critical examination of how the disclosure framework related to financial reporting might be contextualised to Bhutan's ever-shifting digital transformational landscape, a gap that points to the need for further localised research and investigation.

A rapid adoption of digital technologies across financial systems has heightened the exposure of financial institutions to cybersecurity risks. The consequences of cybersecurity incidents for financial reporting remain comparatively unexplored, while prevailing studies have substantially advanced our understanding of cyber risk management, organisational responses, and governance (Cremer et al., 2022 & Adekoya et al., 2025). Besides, as evidenced by Kafi and Akter (2023); Apooyin (2025); and Demchenko (2026), much of this literature concentrates on cybersecurity controls, operational disruptions, and threat mitigation. This gives limited attention to how cyber incidents shape financial reporting decisions such as measurement, recognition, and disclosure of related financial impacts.

Recent studies have begun to examine cybersecurity risk disclosures and the role they play in enhancing transparency and governance. However, the studies identified in this review are situated largely in corporate settings and more established financial and regulatory environments, where reporting requirements, institutional arrangements, and cybersecurity capabilities may differ considerably from those of smaller and developing financial markets (Li et al., 2018; Masoud & Al-Utaibi, 2022; Gao & Calderon, 2025; Singh, 2025). Consequently, the existing literature provides comparatively limited insight into how financial institutions in smaller and developing economies assess, identify, and communicate the financial implications of cybersecurity risks.

Similarly, such limitation carries weight in the Bhutanese context as the existing cybersecurity-related studies and institutional reports in Bhutan have mainly focused on digital resilience, information security capacity, incident response, and cyber threats, rather than on the financial and accounting reporting consequences of cyber incidents (Bhutan Computer Incident Response Team [BtCIRT], 2025). Although Bhutan's financial sector has experienced significant digital transformation and regulatory development (RMA, 2023), limited empirical evidence remains on whether current reporting approaches adequately capture their financial implications and how cybersecurity incidents are reflected in financial reporting practices.

The cybersecurity risk is shaped by organisational capabilities, governance structures, regulatory frameworks, and institutional conditions (Cortez & Dekker, 2022; Opdenbusch, 2025). Considering this, the findings from this review cannot be assumed to fully represent the realities of Bhutan, where the financial institution operates within an aspiring digital transformation, a more concentrated, and a smaller environment.

This study attempts to address an important contextual gap in the cybersecurity-related financial reporting within Bhutan's financial sector through investigating the existing literature. Moreover, this study contributes to the growing cybersecurity and accounting literature and provides practical insights for financial institutions, policymakers, auditors, and regulators seeking to strengthen resilience, accountability, and transparency in the digital financial landscape through gathering evidence from the underrepresented emerging economy.

3. Literature Review

Scholarly, the intersection of cybersecurity breaches and financial reporting integrity has become a focus point in the academic literature, owing to a rapid digital transformation across the global financial sector. Much of the emphasis is on aligning accounting practices with robust cybersecurity measures, which are the most critical aspects of safeguarding data confidentiality and ensuring the reliability of financial statements. Temitayo Oluwaseun Abrahams et al. (2023) coin that strategic integration of accounting and cybersecurity is increasingly recognised as a critical defence against the escalating risks that cyber threats pose to sensitive financial information. Such integration may support accurate financial reporting and transparent disclosure practices, which are vital for maintaining stakeholders' trust and confidence.

3.1. Methodological and Empirical Variance in Loss Measurement

Many previous studies have illustrated the challenges of accounting and measuring losses resulting from cyber incidents. For instance, Adekoya et al. (2025) identify that quantifying the multidimensional impacts of cyberattacks, reputational harm, spanning direct financial losses, and operational disruptions, remains a complex undertaking, largely because no standardised taxonomies exist. A sharp methodological division exists after a critical evaluation of the literature is indicated below:

3.1.1. Direct versus Indirect Loss Recognition

Sharif and Mohammed (2022) highlight the diverse and potentially substantial economic losses associated with cybercrime, where they adopt a broad, literature-based perspective on the financial consequences of cybersecurity incidents. By contrast, Kareem Alsakini et al. (2024) report in their technical accounting literature, placing greater emphasis on the recognition and measurement requirements of the traditional accounting framework, particularly where indirect effects are difficult to quantify reliably.

As a result, this argument exposes an important tension between the broader economic consequences of cyber incidents and the recognition criteria applied within accounting and financial reporting standards.

3.1.2. Methodological Robustness

For methodological robustness, Li et al. (2018) examine the connection between market valuation and cybersecurity disclosures through their empirical studies and offer quantitatively testable evidence mostly grounded in market data and observed disclosure. Methodologically, such studies typically adopt statistical models and robustness checks to assess the consistency of the reported associations; less liquid, with smaller applicability and unlisted financial environments, which may nonetheless be constrained by the characteristics of the study settings and the availability of market-based valuation data. Further, Li et al. (2018) explore cybersecurity risk disclosures in the 10-K filings of U.S. firms within the context of SEC disclosure guidance. However, this market-based approach may have limited applicability to countries such as Bhutan, where the number of listed firms and the availability of market-based valuation data are relatively limited, raising questions about its transferability to the Bhutanese context.

3.2. Disclosure Readability, Corporate Scrutiny, and Disclosure Paradoxes

Over the past few years, accounting disclosure practices related to cybersecurity risks have gained substantial attention among scholars. To comply with the standards and regulatory guidance, numerous studies have depicted that public companies are increasingly disclosing cybersecurity risks in their financial reports despite complexities and challenges involved in responding (Gao & Calderon, 2025; Cortez & Dekker, 2022). On the other hand, a core conflict runs through the literature regarding the efficacy of these disclosures. Singh (2025) demonstrates that while larger firms produce visually lengthy risk disclosures, their structural readability is low and frequently degenerates into boilerplate language designed to shield management from litigation rather than to inform investors. With this finding, Masoud and Al-Utaibi (2022) report a positive correlation between expanded disclosures and audit quality; however, their correlation-based evidence does not establish a causal relationship and contrasts with the argument advanced in the present study. This body of literature is particularly valuable in highlighting this tension, thereby suggesting that expanded voluntary disclosure may, in some cases, function as a defective corporate smokescreen rather than as a mechanism for achieving genuine transparency.

4. Methodology

This study employs a critical systematic review methodology guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 statement with the intention to strengthen methodological transparency, emphasising reproducibility in the identification, screening, selection, and synthesis of relevant literature. The methodological guidance of Snyder (2019) also informs the planning, conduct, and evaluation of the literature review. Systematically, this review process was documented to facilitate an assessment and replication of the methodological procedures. No review protocol was prospectively registered or made publicly available before the commencement of this review process.

4.1. Search Strategy and Parameters

4.1.1. Databases Searched

In this review process, a database search was conducted using Scopus, Web of Science Core Collection, and Business Source Complete (EBSCOhost), in addition to ScienceDirect, which was used to search separately as a publisher platform. In addition, Google Scholar was also used as a supplementary search source; however, only the first eight results from each search were screened, and the screening process was stopped once no additional eligible studies were identified.

4.1.2. Search Window

To identify newly published records meeting the predefined eligibility criteria, the review adopts the publication eligibility period between January 2018 and April 2026. Moreover, the initial literature search was carried out on January 10, 2026, and updated on April 15, 2026, to ensure that the literature review included the most recent and relevant data. Older methodological works, including Morse et al. (2002), are cited to support the review procedure rather than as evidence of cybersecurity-related financial-reporting outcomes.

4.1.3. Search Strings

In this study, some of the key primary search strings included are: data breach; loss recognition; internal controls; financial reporting; accounting disclosure; cyber risk; cybersecurity; IAS 37;

IFRS; developing economies; and emerging markets. Secondary search terms include: bank regulation; central bank oversight; going concern; asset impairment; South Asia; and small state economies.

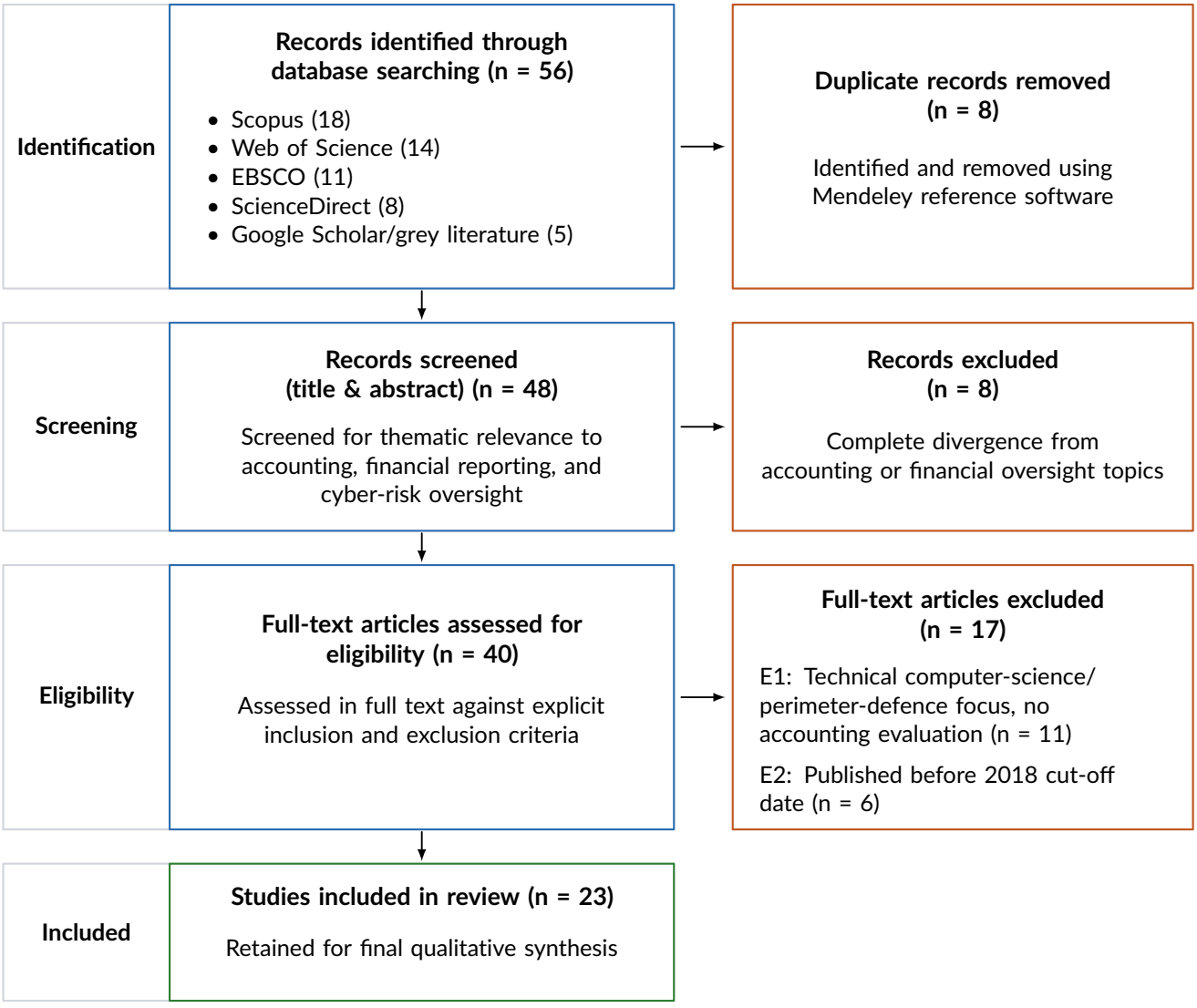
4.2. PRISMA 2020 Selection Protocol and Study Flow

To offer a comprehensive framework for selecting literature in a reproducible and transparent manner, the systematic review was conducted strictly in compliance with the PRISMA 2020 guidelines.

Figure 1 shows the four stages of the selection process through which reports moved: identification; screening; eligibility assessment; and final inclusion in the review.

Figure 1

PRISMA 2020 Flow Diagram of the Systematic Literature Search and Selection Process.



Note. Figure 1 displays the study selection flow. PRISMA = Preferred Reporting Items for Systematic Reviews and Meta-Analyses.

The identification phase yielded 56 records from the predefined information sources, including 18 from Scopus, 14 from Web of Science, 11 from EBSCO, 8 from ScienceDirect, and 5 from supplementary searching through Google Scholar and grey-literature sources.

Mendeley Reference Manager software was used for checking the work duplication. After duplicate removal, 8 records were identified as duplicates and excluded from the list. Only

48 unique records were qualified for screening. Further, during title and abstract screening, 8 records were excluded because they were not substantively relevant to financial reporting, accounting or financial oversight. Therefore, only 40 records for full-text eligibility assessment were qualified.

Although the 2018 publication date limit was applied to the structured database searches, six pre-2018 records identified through supplementary searching and citation chasing were retained because they were potentially relevant to the review question. As a result, these six records were subsequently excluded during full-text assessment because they did not meet the predefined publication-date criterion.

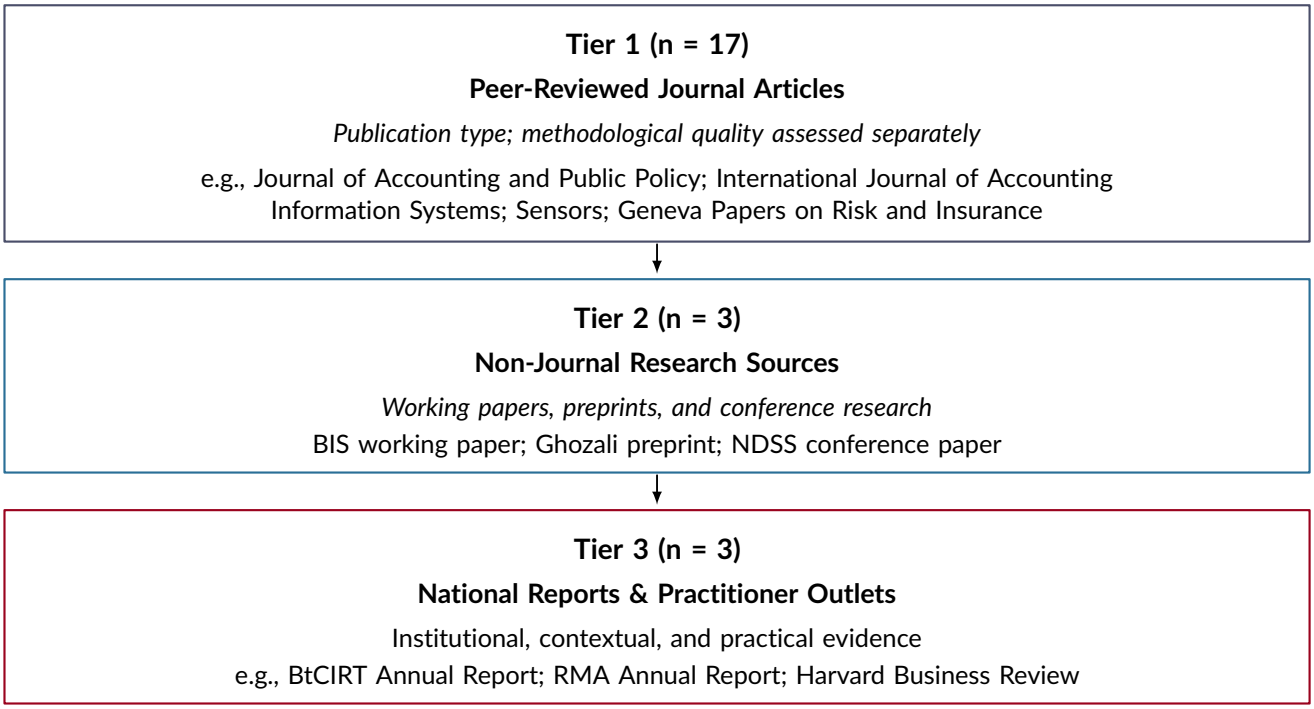
Moreover, 11 records were excluded at the full-text stage because they focused primarily on technical computer science or perimeter defence without evaluating accounting, financial reporting, or related financial oversight outcomes. And 17 records were eliminated at full-text assessment (11 technical-focus exclusions and 6 pre-2018 publications). After this screening process, only 23 studies that met all eligibility criteria were retained for the final qualitative synthesis.

4.3. Source Quality Classification and Evidence Tiering

The 23 sources listed in Table 1 are organised into three descriptive tiers according to the publication type and evidentiary role of the cited version. Tier 1 comprises journal articles, Tier 2 comprises non-journal research, and Tier 3 comprises national institutional reports and practitioner sources. Tier assignment is separate from the assessment of methodological quality and does not establish the validity of a source's findings. Figure 2 presents the resulting distribution of 17, 3, and 3 sources.

Figure 2

Source Classification by Publication Type.



Note. The tiers describe publication types and evidentiary roles, not a descending scale of methodological quality. Source-specific appraisal scores are reported separately in Table 1.

4.3.1. Tier 1: Peer-reviewed journal articles (n=17)

Tier 1 contains the 17 journal sources in Table 1, including empirical studies, literature reviews, conceptual analyses, and methodological guidance. Preprints and conference proceedings are excluded from this category. Where reported, the Chartered Association of Business Schools (CABS) Academic Journal Guide and SCImago Journal Rank (SJR) information describes the publication venue; it does not substitute for assessment of an individual article's design, evidence, or relevance.

4.3.2. Tier 2: Non-journal research sources (n=3)

Tier 2 contains three non-journal research sources: the Bank for International Settlements (BIS) working paper by Abidi et al. (2026), the cited Version 1 preprint by Ghozali (2026), and the conference paper by Opdenbusch (2025). These sources are grouped by publication form, not by a common peer-review status. In particular, the cited Ghozali preprint is not treated as a peer-reviewed journal article. Working papers, preprints, and conference papers are considered with attention to their respective review status, methodological transparency, and contribution to the review objectives.

4.3.3. Tier 3: National reports and practitioner sources (n=3)

Tier 3 contains the RMA annual report, the BtCIRT annual report, and the Harvard Business Review (HBR) article by Huang et al. (2023). The RMA report is classified here because it is an official national institutional report, rather than a research working paper. These three sources provide financial-sector context, technical incident information, and practitioner perspectives. Their authority is assessed in relation to the evidence they provide; institutional or practitioner status alone does not establish methodological quality or justify causal inference.

4.4. Quality Assessment and Study Characteristics

The quality assessment and source characteristics are presented in Table 1. The 1–5 scores express the author's overall appraisal of methodological rigour, source authority, and relevance to the review objectives, with 1 indicating low and 5 indicating high overall quality and usefulness. Methodological rigour concerns the suitability and transparency of the design, evidence, and analysis for the source's purpose; source authority concerns the identifiable publication or issuing institution and the review status of the cited version; and relevance concerns its contribution to cybersecurity-related financial reporting, financial oversight, the Bhutanese context, or the review methodology. These considerations are interpreted in light of the source type, so a national report is assessed for the institutional evidence it supplies. The scores are descriptive judgements reported to one decimal place, not a validated measurement scale or a numerical weighting formula. Source tiers and journal rankings do not determine the scores, and small decimal differences should not be interpreted as precise differences in evidential strength.

Table 1

Summary of Reviewed Literature by Source Tier, Method, and Quality

Study Reference	Source Tier & Ranking	Methodological Design	Primary Focus Area	Quality Score (1–5)
Abidi et al. (2026)	Tier 2 (BIS Working Paper)	Quantitative (Diff-in-Diff)	Cyber Stress Testing & Regulatory Pressure	4.8

Table 1 *(continued)*

Study Reference	Source Tier & Ranking	Methodological Design	Primary Focus Area	Quality Score (1–5)
Adekoya et al. (2025)	Tier 1 (SJR Q1 / WoS)	Systematic Literature Review	Multidimensional Cyber Loss Quantification	4.6
Apooyin (2025)	Tier 1 (Peer-Reviewed)	Qualitative Conceptual	Financial Statement Integrity & Compliance	4.0
BtCIRT (2025)	Tier 3 (National Technical Report)	Institutional Incident Audit	Bhutan Cyber Threat Landscape & IT Gaps	4.2
Cortez & Dekker (2022)	Tier 1 (SJR Q1)	Legal & Governance Analysis	Corporate Governance & Risk Disclosures	4.5
Cram et al. (2023)	Tier 1 (CABS / SJR Q2)	Literature Framework	AIS Research & Cyber Controls	4.4
Cremer et al. (2022)	Tier 1 (SJR Q1 / CABS 2*)	Systematic Literature Review	Cyber Risk Data Availability & Insurance	4.7
Demchenko (2026)	Tier 1 (Peer-Reviewed Journal)	Mixed Methods	Accounting System Continuity & Controls	4.3
Gao & Calderon (2025)	Tier 1 (SJR Q1 / CABS 3*)	Empirical Archival (10-K)	Cyber Governance & SEC Disclosures	4.8
Ghozali (2026)	Tier 2 (Preprint / Empirical)	Quantitative Mixed Methods	ERM & Cyber Fraud Mitigation	4.2
Haryanto (2025)	Tier 1 (Peer-Reviewed Journal)	Qualitative Empirical	Awareness vs Execution Paradox	4.1
Huang et al. (2023)	Tier 3 (Practitioner - HBR)	Case Analysis & Survey	Business Impact & Costs of Cyber Breaches	4.3
Kafi & Akter (2023)	Tier 1 (Peer-Reviewed)	Multiple Case Studies	Accounting Data Protection & Security	4.1
Kareem Alsakini et al. (2024)	Tier 1 (SJR Q3 / WoS)	Quantitative Empirical	Financial Statement Quality & Cyber Risk	4.1
Li et al. (2018)	Tier 1 (SJR Q1 / CABS 3*)	Empirical Archival	Market Valuation & SEC Risk Disclosures	4.9
Masoud & Al-Utaibi (2022)	Tier 1 (SJR Q2)	Empirical Regression	Disclosure Determinants & Audit Quality	4.3
Opdenbusch (2025)	Tier 2 (NDSS Proceedings)	Qualitative In-depth Interviews	Board-Level Decision Making & Bottlenecks	4.7
RMA (2023)	Tier 3 (Central Bank Report)	Macroprudential Audit	Bhutan Financial Sector & Mobile Banking	4.5
Shahzadi et al. (2025)	Tier 1 (SJR Q1 / WoS)	Empirical Experimental	Gamified Cyber Training in Banks	4.5
Sharif & Mohammed (2022)	Tier 1 (Peer-Reviewed)	Systematic Review	Macroeconomic Financial Loss Metrics	4.0
Singh (2025)	Tier 1 (SJR Q2 / CABS 1*)	Empirical Content Analysis	Voluntary Disclosure Readability	4.1

Table 1 *(continued)*

Study Reference	Source Tier & Ranking	Methodological Design	Primary Focus Area	Quality Score (1–5)
Snyder (2019)	Tier 1 (SJR Q1 / CABS 3*)	Methodological Guide	Literature-Review Methodology	4.9
Abrahams et al. (2023)	Tier 1 (Peer-Reviewed)	Critical Literature Review	Strategic Alignment of Accounting & IT	4.1

Note. SJR = SCImago Journal Rank; WoS = Web of Science; CABS = Chartered Association of Business Schools Academic Journal Guide; BIS = Bank for International Settlements; AIS = Accounting Information Systems; ERM = Enterprise Risk Management; SEC = U.S. Securities and Exchange Commission. Quality scores are the author's overall appraisals of methodological rigour, source authority, and relevance (1 = low, 5 = high); they do not follow automatically from tier or journal rank.

4.5. Qualitative Coding Scheme and Single Coder Verification

The coding scheme adopted incorporated both inductive and deductive elements in this reviewing process. As part of the deductive element, seven predefined categories were produced that shaped the initial coding framework of the review process; the BAS and IFRS were employed to draw a priori codes. Subsequently, these were then supplemented by inductive sub-codes developed with the help of the textual analysis of regional policy reports, from which three further thematic categories emerged directly from the data itself in general.

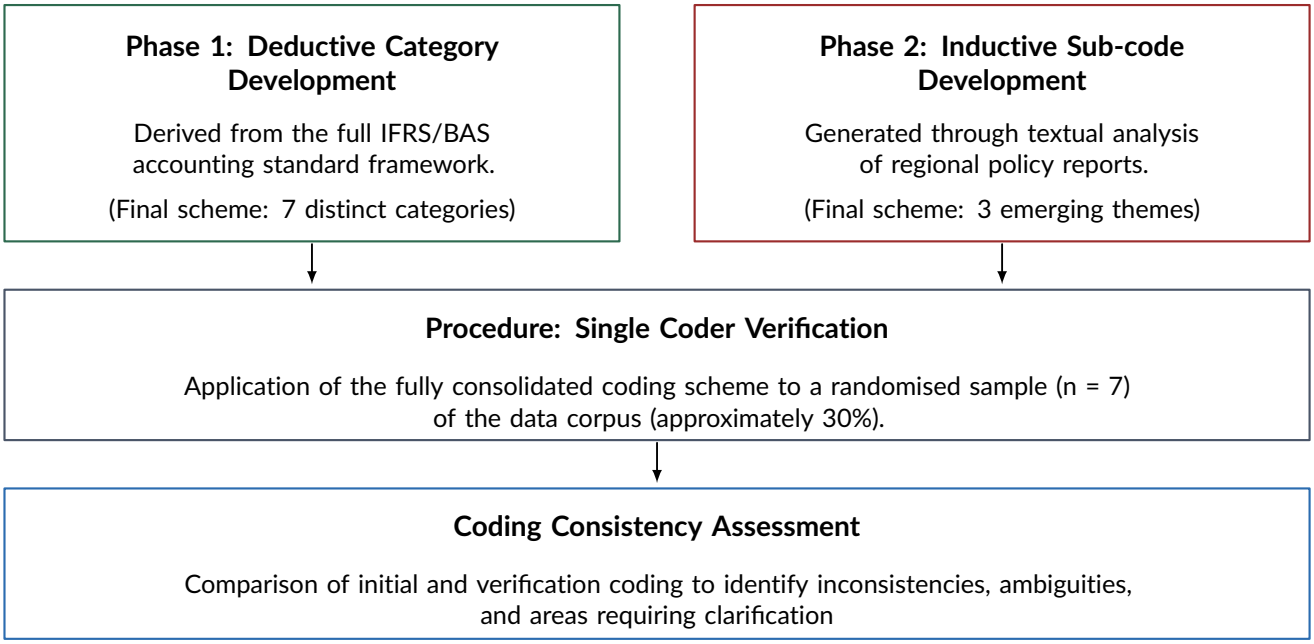
To enhance consistency and dependability of the qualitative analysis, single-coder verification was undertaken. Following the initial coding of all included studies, the researcher independently reapplied the finalized coding framework to randomly selected subsamples of seven studies (approximately 30% of the qualitative sample), consistent with methodological guidance on single-coder verification and coding consistency in systematic and qualitative reviews (Belur et al., 2021; O'Connor & Joffe, 2020; Morse et al., 2002). Figure 3 below explains the deductive coding process and single-coder verification procedure used in the review.

4.6. Deductive–Inductive Coding Framework

The hybrid analytical process ensures both deductive and inductive approaches to integrate thematic categorisation; therefore, the coding framework took shape through these two phases. Under the deductive phase, seven primary categories were drawn from IFRS to generate a priori codes, subsequently mapped directly onto three overarching thematic domains: (a) Measurement (covering Asset Impairment, Loss Contingencies, and Liability Recognition); (b) Disclosure (covering Risk Factors and Materiality Thresholds); and (c) Internal Controls (covering Systemic IT Controls and Audit Committee Oversight). While under the inductive phase, through iterative line-by-line open coding and constant comparative analysis of the qualitative corpus, three distinct sub-themes were derived: (a) reputational capital erosion in relationship banking; (b) nascent central bank regulatory actions; and (c) digital transaction vulnerabilities. These subthemes were derived from the data through inductive analysis. The sub-theme of nascent central bank regulatory actions was extracted from the RMA's Annual Report 2022–23 (RMA, 2023). Reputational capital erosion in relationship banking was identified within the national threat assessment in the BtCIRT Annual Report (2022–2023) (BtCIRT, 2025) and contextualised through South Asian regional reviews by Kafi & Akter (2023) and Kareem Alsakini et al. (2024). Digital transaction vulnerabilities, meanwhile, were derived from regional loss metric syntheses (e.g.,

Figure 3

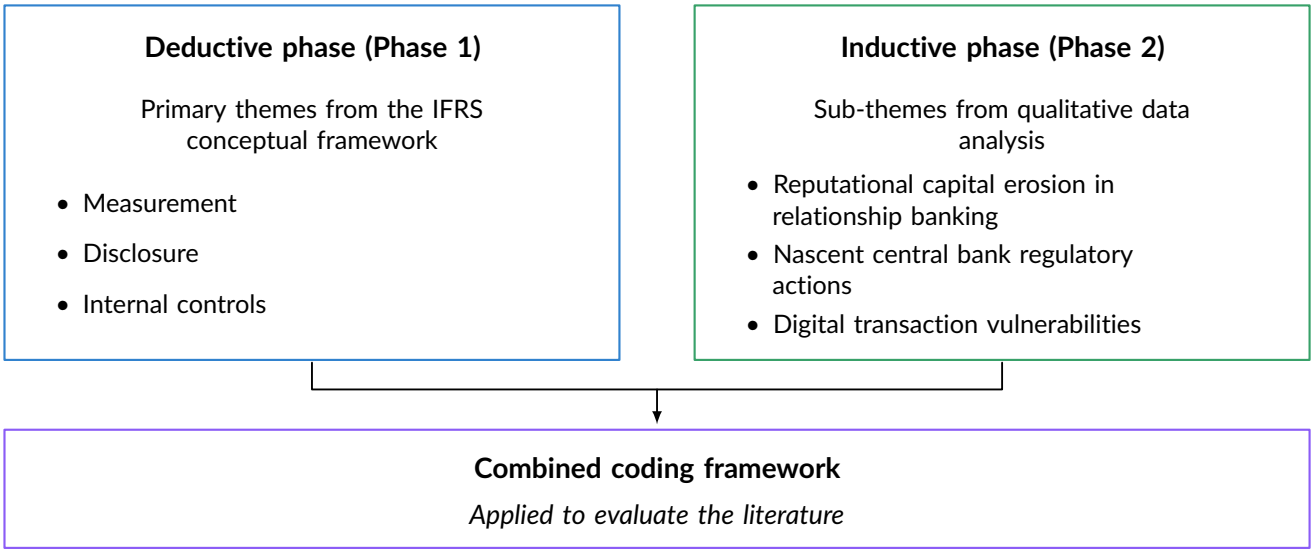
Flow diagram illustrating the integration of deductive and inductive coding approaches, followed by single-coder verification and assessment of coding consistency.



Abidi et al., 2026; Sharif & Mohammed, 2022). The selection process is summarised in the PRISMA flow diagram (Figure 1; Page et al., 2021), the source inventory is presented in Table 1, and complete citations are provided in the reference list. Figure 4 illustrates the structure of the integrated framework.

Figure 4

Development of the Deductive-Inductive Coding Framework; Integrating pre-established standards with nascent qualitative insights



5. Results and Discussion

This section systematically evaluates the seven core accounting mechanisms identified in the research objectives. All the findings presented here have been drawn from the literature patterns (23 reviewed studies), published national incident reports and central bank documentation.

5.1. Systematic Evaluation of Seven Core Accounting Issues

5.1.1. Loss Measurement and Expense Recognition

Under Normative Accounting Theory, the loss measurement and expense recognition are specifically governed to ensure, thereby, the accrual and matching principles reflected in authoritative standards (IAS 1, Presentation of Financial Statements) and IAS 37 (Provisions, Contingent Liabilities and Contingent Assets) (Apooyin, 2025; Frank et al., 2019).

Moreover, it has also been reported that quantifying cyber breaches requires distinguishing direct, immediate operating expenses (for instance, forensic fees, ransom demands, system restoration) from capitalizable expenditures (for instance, infrastructure enhancements yielding future economic benefits under IAS 38), asset impairments (such as derecognition of compromised software under IAS 36), provisions for legal liabilities under IAS 37, and qualitative note disclosures under IAS 1 (Adekoya et al., 2025; Cram et al., 2023).

A general IT operating expense account does not violate accrual or matching principles when a cyber cost's classification is within this expense; however, the expenditure should be recognised in the period in which the service or loss is incurred (Demchenko, 2026; Li et al., 2018). In Bhutan, there is a potential risk or hypothesis that entities may obscure breach costs by absorbing them into routine IT operational budgets without a separate line-item breakdown or note disclosure in case of Bhutan's developing financial ecosystems (BtCIRT, 2025; RMA, 2023). Whereas empirical verification through financial statement analysis or stakeholder interviews remains necessary, such masking, if it exists, would obscure the true fiscal impact of digital disruptions during the period and impair the fair presentation of financial performance (Gao & Calderon, 2025; Kareem Alsakini et al., 2024; Masoud & Al-Utaibi, 2022).

5.1.2. Asset and Liability Volatility

In Normative Accounting Theory, asset and liability volatility are monitored and operationalised through key financial reporting standards: (a) IAS/BAS 36-Impairment of Assets; (b) IAS/BAS 38-Intangible Assets; and (c) IAS/BAS 37 -Provisions, Contingent Liabilities and Contingent Assets. Typically, cyber incidents can weaken core database infrastructure and adversely affect capitalised software assets. There are objective indicators of impairment, including a serious system breach, technological obsolescence, and significant operational disruption. Therefore, entities are required to assess whether the asset's carrying amount exceeds its recoverable amount in this case under IAS/BAS 36. Similarly, on the liability side, IAS/BAS 37 requires a provision for a cyber breach when a past event creates a present legal or constructive obligation, an outflow of economic resources is probable, and the amount can be estimated reliably. Failure to recognise a qualifying provision, or to disclose a contingent liability when required, could materially distort the statement of financial position (Apooyin, 2025; Demchenko, 2026; Kareem Alsakini, 2024).

5.1.3. Disclosure Adequacy

The Stakeholder Theory, which highlights depositor trust and transparency, is directly associated with disclosure adequacy. Likewise, it has been reported that corporate disclosure in emerging banking sectors often relies on boilerplate narrative descriptions of generic IT risk (Singh, 2025; Haryanto, 2025). Therefore, the evidence supports that even without structured quantitative and qualitative reporting parameters, financial users such as investors, international development partners, depositors, and counterparties could not exactly assess an institution's cyber risk posture as well as financial preparedness in detail. Empirical evidence from a previous study (Li et al., 2018) on developed market regulatory mandates on how to use SEC disclosure guidance and Cram et al. (2023) on accounting information systems research frameworks indicate

standardised disclosure on maintaining more transparency in the reporting system. Nonetheless, these structured parameters remain largely absent as a digital financial system emerges.

5.1.4. Internal Control Effectiveness

Under Agency Theory, most executive oversight and stakeholder governance are highlighted with special focus on aligning principal and agent interests. In Bhutan, a rapid adoption of digital payment gateways and mobile banking platforms; (a) mPAY (Bhutan National Bank), (b) ePay (Bhutan Development Bank), (c) eTeeru (Tashi Bank), and (d) mBoB (Bank of Bhutan) are some examples of how financial institutions are expanding the operational attack surface (RMA, 2023; BtCIRT, 2025).

Therefore, the internal control framework faces potentially systemic vulnerabilities and risks, exacerbating agency costs and compromising data integrity, if all automated digital transaction logs are not continuously reconciled with the core financial ledgers through an independent IT expert and financial audit trails. Relevant assurance and auditing standards include (a) ISAE 3402 Assurance Reports on Controls at a Service Organisation and (b) ISA 315 (Identifying and Assessing the Risks of Material Misstatement). Controls to address these risks may include rigorous logical access controls, independent dual key verification, and continuous automated reconciliation protocols. Consequently, these controls can support executive oversight and ledger alignment (Apooyin, 2025; Cram et al., 2023).

5.1.5. Insurance Coverage Recognition

The Normative Accounting Theory, which is operationalised through IAS/BAS 37 (Provisions, Contingent Liabilities and Contingent Assets), enshrines the insurance coverage recognition in the financial reporting standard. To be more specific, this standard states that a potential insurance recovery which is not tied to an existing provision is classified as a contingent asset, but cannot be recognised in the financial statements unless inflow of economic benefits becomes virtually certain and valid. Regarding the entity recognising a provision for cyber breach, any reimbursement from an insurance policy is recognised as a separate asset only when it is virtually certain that this will be received after the settlement of the entity's obligation (with the recognised reimbursement capped at the amount of the provision). However, in most developing cyber insurance markets with limited local underwriting capacity, treating it as an anticipated insurance claim (immediate offsets against realised operational cyber losses) before meeting the virtual certainty threshold would violate standard presentation rules and might even lead to the premature recognition of assets on the financial position statements (Cremer et al., 2022).

5.1.6. Going Concern Assessments

In an accounting system, the going concern is categorised under Normative Accounting Theory and Auditing Standards known as ISA 570 (revised going concern). While implementing this standard, the management team is responsible for assessing the entity's going concern; in particular, the auditor is responsible for evaluating management's tasks related to the assessment of determining the existence of material uncertainties to the entity's ability to survive in the long term. Most operational events or conditions, such as: (a) the loss of core credit ledgers without functional off-site backups; (b) severe ransomware incidents; and (c) catastrophic ledger corruption that might cause significant doubt on a smaller financial entity's ability to continue as a going concern, are the main concerns. Although a cyber incident does not automatically invalidate going concern status, it creates operational paralysis and therefore, management should validate and account for forward-looking viability assessment. Additionally, external auditor procedures

should incorporate cyber stress scenarios into their formal risk assessment proposals to evaluate management's operational continuity assumptions and future financial plan (Abidi et al., 2026).

5.1.7. Regulatory Compliance and Penalty Provisioning

Agency Theory and primary accounting standards (IAS/BAS 37: Provisions, Contingent Liabilities and Contingent Assets) and (IAS/BAS 10: Events After the Reporting Period) are directly related to regulatory penalties in the accounting system. Similarly, all financial institutions operate under regulatory oversight from the RMA (2023). Under IAS/BAS 37, an entity recognises a provision for a cyber breach or related regulatory penalty when a past event has created a present legal or constructive obligation, settlement will probably require economic resources, and the amount can be estimated reliably. A possible obligation, or a present obligation that fails either the probability or reliable-estimation condition, is treated as a contingent liability. Such an exposure is disclosed in the notes unless the prospect of an outflow is remote; it is not recognised as a liability in the statement of financial position (IFRS Foundation, n.d.-d).

Under IAS/BAS 10, regulatory or penalty developments occurring after the reporting date but before the financial statements are authorised for issue must be assessed according to the conditions they evidence. Where they provide evidence of conditions existing at the reporting date, the entity adjusts the financial statements as necessary, including recognising or revising a provision when the IAS/BAS 37 criteria are met. Developments arising from new conditions after the reporting date are non-adjusting events; if material, their nature and estimated financial effect must be disclosed, or the entity must explain that the effect cannot be estimated. Cybersecurity-related fines therefore cannot be treated automatically as post-reporting-date disclosures: their recognition and disclosure depend on the underlying obligation, the reporting-date conditions, and materiality (IFRS Foundation, n.d.-b).

5.2. Contextual and Institutional Boundaries: Respective Responsibilities of Financial Standard-Setters and BtCIRT

5.2.1. BtCIRT Operational Scope

In the Bhutanese context, BtCIRT, which operates under the Cybersecurity Division of the Government Technology Agency (GovTech), acts as a national custodian to monitor technical incidents and threats as a response body to provide cyber threat advisories, technical incident coordination, and public security awareness. Besides, the BtCIRT also collects security reports and technical incident logs; nonetheless, fundamentally, technical incident response information serves a different purpose than financial-related evidence, which is necessary for financial reporting. On top of that, BtCIRT records themselves may not align and fulfil the accounting requirements, such as measurement, faithful presentation under the required reporting standards and recognition; however, it might inform and support an entity's assessment and evaluation.

5.2.2. Financial Reporting Authority

In Bhutan, the financial reporting integrity is supported by the Accounting and Auditing Standards Board of Bhutan (AASBB), the RMA, and external auditors within their respective statutory mandates. These respective regulatory and professional bodies are responsible for ensuring the reporting standards and relevant standard-setting and regulating ethics in accounting reports.

In accordance with the applicable financial reporting standard, records of technical breaches or control failures should not be accounted for as accounting provisions themselves. Rather, such records provide relevant evidence for evaluating whether the underlying events or conditions have implications for the presentation, recognition, measurement or disclosure of financial

information. Therefore, the appropriate accounting treatment should be determined through the established financial reporting supported by a regulatory framework, rather than through an automatic conversion of technical breach records into accounting provisions.

5.2.3. Central Bank Macroprudential Oversight Scope

For regulating and supervising financial institutions in Bhutan, the RMA is mandated and responsible for establishing prudential, risk management, cybersecurity, and related regulatory requirements. Nevertheless, the implementation of these requirements remains the responsibility of each financial institution through its executive management and board of directors. They are accountable for managing business risk, operational security, institutional governance, as well as effective internal mechanisms. Also, independently, both external and internal audit functions support the effectiveness of these controls and assure their adequacy, but are more consistent with the professional requirements and applicable regulatory requirements.

In particular, the day-to-day prevention, detection, management, and remediation of cybersecurity and operational risks remain the responsibility of the regulated institution, while the RMA's role is primarily supervisory and regulatory.

6. Actionable Implementation Roadmap

This critical review identifies how cybersecurity breaches act as a potentially significant risk to financial reporting integrity within Bhutan. Most findings of the review indicate that cybersecurity incidents and related control weaknesses may have financial reporting implications beyond the immediate technical or operational effects. In accounting, the key effects include: availability of financial information, accuracy, reliability, and completeness.

In Bhutan, these vulnerabilities should be understood as potential material financial-reporting risks and control weaknesses, in the absence of sufficient primary Bhutanese incident-level and financial statement evidence, rather than as established accounting failures or demonstrated distortions of asset values and liabilities. Therefore, strengthening institutional resilience requires a coordinated approach to internal controls, risk management, financial reporting, assurance, and cybersecurity governance. The following phased roadmap and prioritised recommendations are made based on the documented findings of this review.

6.1. Short-Term Actions (0–12 Months).

The study recommends RMA and AASBB, within their respective statutory mandates, to develop additional guidance on the financial-reporting implications of material cybersecurity incidents, aligning with Bhutan's existing BAS/IFRS framework.

This kind of guidance could promote greater consistency in terms of quantitative and qualitative disclosure of material cyber incidents, mostly the consequential financial effects and remediation costs; however, encompassing aggregation principles, safeguards, and materiality thresholds against financial disclosures of the institutions might further expose them to high cybersecurity risks. Similarly, the guideline should also clarify how existing financial reporting requirements incorporate the matters related to cyber and its legal basis (regulatory and contractual obligations), including compensation claims, provisions, contingent liabilities, and penalties arising from cybersecurity incidents. In particular, these institutions may explain and adopt the IFRS requirements and application of BAS 37 in the Bhutanese context, instead of treating IAS 37 and BAS 37 as separate parallel standards. Thus, any new compliance arrangements and supervision should always remain in conjunction with the existing statutory and regulatory framework of the country.

6.2. Medium-Term Actions (1–3 Years)

The second recommendation is related to the term between 1 and 3 years, where the institutions need to assess the feasibility of a structured capacity-building framework for integrating IT and financial-audit competencies among local audit professionals. The assessment could examine the appropriate competent authority, legal and institutional basis, the potential costs of implementation, resource and capacity requirements, delivery arrangements, and the target professional groups.

For developing competency requirements and continuing professional development (CPD), collaboration with the relevant standard-setting and professional bodies like AASBB should be given opportunities in framing digital financial-system controls, cyber-risk assessment, and IT general controls (ITGC) in Bhutan. After a feasibility assessment, a formal certification pathway could be considered if evidence demonstrates that professional certification provides greater assurance of auditor competency.

6.3. Long-Term Actions (3+ Years)

The final recommendation is related to the long-term actions, which are more than three years. It explores the integration of cybersecurity-related competencies into relevant accounting and auditing programmes, which indeed is subject to the curriculum approval requirements of the relevant professional bodies and higher education in Bhutan.

Taking into account the reviewed evidence regarding the gaps in digital financial controls, cybersecurity awareness, and its risk assessment, curriculum development could embed learning outcomes directly associated with: evaluating ITGC, identifying cyber-related financial risks, assessing the potential financial-reporting implications of cybersecurity incidents, and interpreting its risk indicators. Moreover, appropriate case-based learning could be used to connect cybersecurity events with accounting, internal control, audit, and financial-reporting considerations. Implementation could be evaluated through curriculum review, stakeholder feedback, student competency assessments, and periodic assessment of graduate preparedness for technology-related audit and financial-reporting risks. The recommendation should therefore be treated as a longer-term capacity-building measure informed by the identified skills and control gaps in the reviewed literature, rather than as an immediate structural requirement for all higher education accounting programmes.

7. Limitations and Future Research Directions

This critical review has some methodological limitations. First, the relatively small review corpus limits the breadth and representativeness of the available evidence. The evidence base may also be subject to database coverage, language, publication, and grey-literature biases, potentially resulting in relevant studies or institutional documents being overlooked. The inclusion of heterogeneous evidence types, including empirical studies, regulatory and policy documents, and other published sources, further limits direct comparability across the evidence. In addition, the classification, tiering, and coding of the reviewed evidence involved researcher judgement and may therefore introduce a degree of subjectivity.

A further limitation is the limited availability of primary empirical evidence from Bhutan on the financial-reporting consequences of cybersecurity incidents. The review corpus also contained limited publicly available material on corporate cybersecurity and financial-reporting disclosure; consequently, the review does not provide a basis for assessing the overall extent or prevalence of voluntary disclosure among Bhutanese corporations. The reliance on accessible published and institutional sources may likewise have resulted in relevant studies, unpublished

evidence, or institution-level grey literature being missed. Where a review protocol was not prospectively registered, this also limits the transparency and reproducibility of the review process.

Accordingly, the findings should be interpreted as an evidence-informed synthesis of the available literature and regulatory material rather than as establishing causal relationships, the prevalence of cybersecurity-related financial-reporting failures, or the effectiveness of specific practices within Bhutanese institutions. Particularly, these limitations matter while interpreting what international evidence implies for the Bhutanese context, where technological conditions, regulatory, and institutional factors may differ. Nonetheless, the synthesis offers a basis for identifying potential financial reporting risk, control vulnerabilities, and areas that warrant further empirical investigation in the future. Drawing on the reviewed evidence concerning the future demand for additional research, the following areas are to be prioritised:

1. Examining actual cyber incidents and how they are treated in financial reporting within Bhutanese financial institutions (with appropriate confidentiality protections), to develop empirically grounded case studies and identify implementation challenges.
2. Conducting comparative, regional case-study research that contrasts Bhutan's regulatory responses and accounting practices with those of geographically analogous South Asian nations (e.g., Nepal, Maldives, Sri Lanka), to establish localised best practices tailored to small, developing economies.
3. Deploying structured, anonymised survey instruments and semi-structured interviews with the relevant RMA Officials, Chief Financial Officers (CFOs), external audit partners and internal auditors, to devise baseline technical preparedness, additional support needed, and perceived barriers to cyber-risk disclosure to implement new accounting frameworks.

In the context of Bhutan's ongoing digital transformation, this systematic review identifies cybersecurity as a relevant financial-reporting and governance risk. The reviewed evidence points to potential linkages across internal control vulnerabilities, integrity, availability of financial information, and cybersecurity weaknesses. Even though in Bhutan, the specific empirical evidence remains limited, these relationships cannot be read as established financial-reporting failures or causal effects within Bhutanese financial institutions. Instead, the international evidence and regulatory literature reviewed here are interpreted for the Bhutanese context, and they provide a basis for considering strengthened cyber-risk disclosure, control assurance, and accounting and auditing competencies within the existing financial-reporting framework. Therefore, the proposed measures are all relevant policy and capacity-building recommendations derived from the identified evidence gaps and risks, rather than established outcomes of cybersecurity reform. Thus, their applicability to other small and developing economies stands as a proposition for future comparative research, which requires empirical testing across different institutional, regulatory, and technological contexts.

References

Abidi, N., Gambacorta, L., Kok, C., Madio, L., Miquel-Flores, I., & Partida, A. (2026). *Disciplining digital risk: Evidence from cyber stress tests* (BIS Working Papers No. 1351). Bank for International Settlements. https://www.bis.org/publ/work1351.htm

Adekoya, O. A., Atlam, H. F., & Lallie, H. S. (2025). Quantifying the multidimensional impact of cyber attacks in digital financial services: A systematic literature review. *Sensors*, *25*(14), Article 4345. https://doi.org/10.3390/s25144345

Apooyin, A. E. (2025). The impact of cybersecurity on financial reporting: Strengthening data integrity and regulatory compliance. *International Journal of Science and Research Archive*, *14*(2), 626–637. https://doi.org/10.30574/ijsra.2025.14.2.0427

Belur, J., Tompson, L., Thornton, A., & Simon, M. (2021). Interrater reliability in systematic review methodology: Exploring variation in coder decision-making. *Sociological Methods & Research*, *50*(2), 837–865. https://doi.org/10.1177/0049124118799372

Bhutan Computer Incident Response Team. (2025). *BtCIRT annual report (2022–2023)*. https://btcirt.bt/wp-content/uploads/2025/04/BTCIRT-Annual-Report-2022-2023.docx.pdf

Cortez, E. K., & Dekker, M. (2022). A corporate governance approach to cybersecurity risk disclosure. *European Journal of Risk Regulation*, *13*(3), 1–23. https://doi.org/10.1017/err.2022.10

Cram, W. A., Wang, T., & Yuan, J. (2023). Cybersecurity research in accounting information systems: A review and framework. *Journal of Emerging Technologies in Accounting*, *20*(1), 15–38. https://doi.org/10.2308/JETA-2020-081

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance—Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Demchenko, T. (2026). The impact of cyber risks on the functioning of the accounting system and their management. *Oblik i Finansi*, *2*(112), 44–52. https://doi.org/10.33146/2518-1181-2026-2(112)-44-52

Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems*, *33*(3), 183–200. https://doi.org/10.2308/isys-52374

Gao, L., & Calderon, T. G. (2025). Cybersecurity risk governance and companies' cybersecurity risk disclosures in their 10-K filings. *Journal of Accounting and Public Policy*, *54*, Article 107376. https://doi.org/10.1016/j.jaccpubpol.2025.107376

Ghozali, I. (2026). *Enterprise risk management and cyber fraud mitigation: Evidence from Indonesian state-owned enterprises* (Preprints No. 202603.0965, Version 1). Preprints. https://www.preprints.org/manuscript/202603.0965/v1/download

Haryanto, H. (2025). Cybersecurity paradox in MSMEs: Imbalance of awareness and implementation in the digital era. *East Asian Journal of Multidisciplinary Research*, *4*(1), 143–156. https://ejeset.saintispub.com/ejeset/article/download/470/120

Huang, K., Wang, X., Wei, W., & Madnick, S. (2023, May 22). The devastating business impacts of a cyber breach. *Harvard Business Review*. https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

IFRS Foundation. (n.d.-a). *IAS 1 Presentation of financial statements*. https://www.ifrs.org/issued-standards/list-of-standards/ias-1-presentation-of-financial-statements/

IFRS Foundation. (n.d.-b). *IAS 10: Events after the reporting period*. https://www.ifrs.org/issued-standards/list-of-standards/ias-10-events-after-the-reporting-period/

IFRS Foundation. (n.d.-c). *IAS 36 Impairment of assets*. https://www.ifrs.org/issued-standards/list-of-standards/ias-36-impairment-of-assets/

IFRS Foundation. (n.d.-d). *IAS 37: Provisions, contingent liabilities and contingent assets*. https://www.ifrs.org/issued-standards/list-of-standards/ias-37-provisions-contingent-liabilities-and-contingent-assets/

IFRS Foundation. (n.d.-e). *IAS 38 Intangible assets*. https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/

International Auditing and Assurance Standards Board. (2009). *Staff overview: International Standard on Assurance Engagements (ISAE) 3402, Assurance reports on controls at a service organization*. https://www.iaasb.org/publications/staff-overview-international-standard-assurance-engagements-isae-3402-assurance-reports-controls

International Auditing and Assurance Standards Board. (2015). *International Standard on Auditing (ISA) 570 (Revised), Going concern*. https://www.ifac.org/system/files/publications/files/ISA-570-(Revised).pdf

International Auditing and Assurance Standards Board. (2019). *ISA 315 (Revised 2019): Identifying and assessing the risks of material misstatement*. https://www.iaasb.org/publications/isa-315-revised-2019-identifying-and-assessing-risks-material-misstatement

Kafi, M., & Akter, N. (2023). Securing financial information in the digital realm: Case studies in cybersecurity for accounting data protection. *American Journal of Trade and Policy*, *10*(1), 15–26. https://doi.org/10.18034/ajtp.v10i1.659

Kareem Alsakini, S. A., Ali Alawawdeh, H., & Alsayyed, S. (2024). The impact of cybersecurity on the quality of financial statements. *Applied Mathematics & Information Sciences*, *18*(1), 169–181. https://doi.org/10.18576/amis/180117

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

Masoud, N., & Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. *Research in Economics*, *76*(2), 131–140. https://doi.org/10.1016/j.rie.2022.07.001

Ministry of Finance. (n.d.). *Accounting and Auditing Standard Boards of Bhutan*. https://mof.gov.bt/pages/accounting-and-auditing-standard-boards-of-bhutan/

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification Strategies for Establishing Reliability and Validity in Qualitative Research. *International Journal of Qualitative Methods*, *1*(2), 13–22. https://doi.org/10.1177/160940690200100202

O'Connor, C., & Joffe, H. (2020). Intercoder reliability in qualitative research: Debates and practical guidelines. *International Journal of Qualitative Methods*, *19*, 1–13. https://doi.org/10.1177/1609406919899220

Opdenbusch, J. C. (2025). "Where are we on cyber?" A qualitative study on boards' cybersecurity risk decision making. *Proceedings of the Network and Distributed System Security (NDSS) Symposium*, 1–18. https://www.ndss-symposium.org/wp-content/uploads/2025-595-paper.pdf

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, *372*, Article n71. https://doi.org/10.1136/bmj.n71

Royal Monetary Authority of Bhutan. (2023). *Annual report 2023*. https://www.rma.org.bt/media/news_upload/Annual%20Report%202022-23.pdf

Shahzadi, A., Ishaq, K., Nawaz, N. A., Rosdi, F., & Khan, F. A. (2025). Unveiling personalized and gamification-based cybersecurity risks within financial institutions. *PeerJ Computer Science*, *11*, Article e2598. https://doi.org/10.7717/peerj-cs.2598

Sharif, M. H. U., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cybersecurity and future trends. *World Journal of Advanced Research and Reviews*, *15*(1), 138–156. https://doi.org/10.30574/wjarr.2022.15.1.0573

Singh, H. (2025). Voluntary cybersecurity risk disclosures and firms' characteristics: The moderating role of the knowledge-intensive industry. *Asian Journal of Accounting Research*, *10*(2), 168–185. https://doi.org/10.1108/AJAR-12-2023-0413

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Temitayo Oluwaseun Abrahams, Sarah Kuzankah Ewuga, Kaggwa, S., Prisca Ugomma Uwaoma, Azeez Olanipekun Hassan, & Samuel Onimisi Dawodu. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. *World Journal Of Advanced Research and Reviews*, *20*(3), 1743–1756. https://doi.org/10.30574/wjarr.2023.20.3.2691

Declarations

AI Use Declaration

The author declares that AI tools such as Claude AI and Grammarly were used in this study solely to assist with grammatical corrections. All research components, including the research design, visuals, analysis, interpretation, and conclusions presented in this study, are the author's own original work. No AI was used to fabricate content or alter results to mislead readers. The author takes full responsibility for the accuracy, integrity, and originality of this work.

Competing Interests

The author declares that there are no competing interests to disclose in relation to this study.

Acknowledgements

The author would like to express sincere gratitude to Mr. Sonam Wangda, Lecturer, Gedu College of Business Studies, Royal University of Bhutan, for his guidance on the manuscript preparation and review process.

Funding

This research received no financial support, grant, or sponsorship from any organisation, institution, or individual.