

Article

Cybersecurity Governance Deficiencies in External Audit: A Structured Review and Control-to-Assertion Framework

Alessio Faccia ^{1,*}  and Somkiat Tangjitsitcharoen ²¹ School of Business, University of Birmingham Dubai, Dubai P.O. Box 341799, United Arab Emirates² Department of Industrial Engineering, Faculty of Engineering, Chulalongkorn University, Phayathai Road, Patumwan, Bangkok 10330, Thailand; somkiat.ta@eng.chula.ac.th

* Correspondence: a.faccia@bham.ac.uk

Abstract

Digital financial reporting depends on identity services, enterprise systems, cloud platforms, automated controls and system-generated evidence. Cybersecurity weaknesses therefore enter external audit when a governance condition or control deficiency affects a material reporting process, an assertion, a disclosure, an estimate or the reliability of audit evidence. This article develops a non-deterministic control-to-assertion framework through a structured integrative review. The search, completed on 16 July 2026, covered English-language journal work published from 2000 to 15 July 2026 through Google Scholar and publisher search services. The final analytic set contains 32 peer-reviewed journal articles, four institutional sources and two public company filings used for worked application. The revision separates organisation-level cybersecurity governance deficiencies from process-level cyber control deficiencies. It also locates the model against COSO, COBIT 2019, NIST CSF 2.0, IT general control methods and relevant International Standards on Auditing. Existing sources provide taxonomies for governance, internal control, security outcomes and audit procedures. The new framework supplies the missing translation route between those taxonomies: governance condition, control state, financial reporting dependency, assertion-level misstatement risk, audit-evidence reliability, audit response and reassessment. Compensating, detective and corrective controls might interrupt or reduce the route, so no governance deficiency automatically produces a control failure or a material misstatement. Two worked documentary applications, The Clorox Company and MGM Resorts International, show how public incident facts enter account, assertion, evidence and procedure analysis. The framework does not estimate incident probability, expected loss or a cyber risk score. It provides a file-ready reasoning structure for entity-specific risk assessment under the auditing standards. Its main contribution lies in the separate treatment of misstatement risk and evidence reliability, followed by a traceable link to accounts, assertions, evidence sources, specialist input and audit procedures.



Academic Editor: Sokratis Katsikas

Received: 16 July 2026

Accepted: 28 July 2026

Published: 3 August 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

Keywords: cybersecurity governance; external audit; financial reporting; internal control; audit evidence; IT general controls; assertions; risk assessment; service organisations

1. Introduction

Financial reporting now relies on enterprise resource planning systems, cloud applications, payment channels, data interfaces, automated calculations and outsourced service providers. Cyber incidents and weak security controls therefore matter to external auditors when they affect transaction processing, accounting records, estimates, disclosures or

system-generated evidence. Accounting and information-system research links cybersecurity events with disclosure, internal control, audit pricing, audit quality, board oversight and organisational response [1–4].

Prior research nevertheless stops at different points in the audit reasoning process. Governance studies examine board structures and cyber reporting [5–9]. Disclosure studies examine content, determinants and regulatory response [10–16]. Internal-control studies examine breach consequences, control weaknesses and remediation [17–24]. Audit studies examine fees, effort and audit-quality outcomes [25–29]. Work on organisational response examines reputation, management action and post-incident learning [30–32]. Each stream supports part of the route from cyber governance to audit work. Few studies specify the full route from an organisation-level governance condition to a process-level control state, a material financial reporting dependency, a financial statement assertion, an evidence-reliability issue and a documented audit response.

Professional frameworks solve adjacent problems. COSO supplies an internal-control structure. COBIT 2019 supplies governance and management objectives for information and technology. NIST CSF 2.0 supplies security outcomes across Govern, Identify, Protect, Detect, Respond and Recover. IT general control methods focus on access, program change, computer operations and related domains. The International Standards on Auditing govern risk identification, responses, evidence, service organisations, estimates, subsequent events, going concern and specialist work [33–36]. None of these sources, used alone, provides a single audit-file crosswalk from cyber governance evidence to account-level and assertion-level work.

The earlier manuscript described this missing connection as fragmentation. Review comments rightly identified a need for more precision. Mere reorganisation of established ideas would offer limited research value. The revised article therefore states a narrower contribution. It does not introduce a new cybersecurity taxonomy, internal-control model or audit standard. It introduces a translation architecture linking established governance, control and audit constructs, with two separate audit consequences: risk of material misstatement and reduced reliability of audit evidence.

Conceptual precision also requires a distinction between governance and controls. A cybersecurity governance deficiency is an organisation-level weakness in direction, oversight, accountability, risk ownership, reporting, resource allocation, third-party oversight or remediation. A cyber control deficiency is a process-level weakness in control design, implementation, operation or monitoring. The two constructs sit at different organisational levels. A governance deficiency might increase the chance of weak controls, yet the relationship is not automatic. Strong compensating controls might lower residual risk. Sound governance might coexist with an isolated operating failure. Corrective action might interrupt the route before financial reporting is affected.

This study addresses three research questions. RQ1 asks how prior accounting, information-system and audit research links cybersecurity governance, cyber controls, financial reporting and external audit. RQ2 asks how established professional frameworks differ from and connect with an audit-specific translation model. RQ3 asks how an auditor might document the route from a cyber condition to accounts, assertions, evidence reliability and audit work without assigning unsupported numerical scores.

A structured integrative review answers the questions. The method reports search sources, dates, search blocks, eligibility rules, screening logic, coding categories and synthesis steps. Official standards and public filings form separate documentary sets. The design excludes interviews because the present question concerns conceptual integration and public traceability. Interviews would require a distinct field study, participant sampling, ethics

approval and access to confidential audit material. Vendor commentary remains outside the evidence set because commercial framing and uneven provenance reduce reproducibility.

Two public filings provide worked applications. The Clorox Company filing describes an incident that disrupted automated order processing, required manual procedures and interim controls, affected net sales and earnings and produced recovery costs partly offset by insurance [37]. MGM Resorts International reported property disruption, an estimated USD 100 million effect on Adjusted Property EBITDAR and less than USD 10 million in one-time costs while reporting no expected material annual effect on financial condition and results [38]. The applications test usability and boundary discipline. They do not constitute empirical validation.

The article proceeds in seven parts. Section 2 defines the constructs and locates the model against recognised frameworks. Section 3 reports the review method. Section 4 synthesises the evidence. Section 5 presents the revised non-deterministic model, traceability protocol and expanded mapping matrix. Section 6 applies the model to public filings. Section 7 discusses contribution, standards, materiality, probability, limits and further research. Section 8 concludes.

2. Conceptual and Professional Positioning

2.1. Cybersecurity Governance, Financial Reporting and External Audit

Cybersecurity governance concerns decision rights and accountability for cyber risk. Relevant features include board oversight, management ownership, risk appetite, reporting lines, escalation rules, resources, third-party governance and remediation follow-up. External audit does not assess these features as a free-standing security assurance engagement. Audit interest begins when governance evidence bears on the control environment, the entity risk-assessment process, the information system relevant to financial reporting, disclosure controls or management response to incidents, the construct definitions and audit boundaries are presented in Table 1.

Table 1. Construct definitions and audit boundaries.

Construct	Definition	Illustrative Condition	Audit Meaning
Cybersecurity governance deficiency	Organisation-level weakness in direction, oversight, accountability, risk ownership, reporting, resources, third-party oversight or remediation.	Board reporting omits financial reporting effects. Risk ownership is unclear. Policy approval lacks follow-up. Material incidents do not reach the audit committee.	Evidence about the control environment and entity risk assessment. It does not prove a process-level control failure.
Cyber control deficiency	Process-level weakness in control design, implementation, operation or monitoring.	Privileged access is not reviewed. Production changes lack approval. Recovery tests fail. Security logs are incomplete.	Possible effect on assertions, automated controls, reports, populations or source data.
Cyber incident	Observed event involving unauthorised access, disruption, data loss, manipulation, extortion or service failure.	Ransomware, payment diversion, cloud outage or unauthorised system access.	A risk indicator and possible accounting event. An incident alone does not prove a material misstatement.

Table 1. *Cont.*

Construct	Definition	Illustrative Condition	Audit Meaning
Financial reporting dependency	Reliance of a material process, account, disclosure, estimate or audit procedure on a system, service, dataset or control.	Revenue interface, payroll processor, inventory-costing engine, consolidation tool or incident-loss estimate.	Determines whether a cyber matter enters financial statement audit scope.
Misstatement risk	Possibility of a material error or fraud at financial-statement or assertion level.	Fictitious journals, incomplete revenue, wrong valuation, omitted provision or inadequate disclosure.	Assessed through likelihood and magnitude under ISA 315, followed by responses under ISA 330.
Evidence-reliability risk	Possibility of incomplete, altered, unavailable or weakly controlled information used in audit work.	Unreliable logs, incomplete transaction populations, corrupted reports or unavailable records.	Affects source reliability, population completeness, controls reliance and the need for independent evidence.
Residual cyber-audit risk	Risk remaining after compensating, detective or corrective controls and planned audit work.	Manual control compensates for an unavailable automated control. Recovery work restores complete records.	Requires reassessment rather than an automatic pass-through from governance to misstatement.

Financial reporting dependency forms the bridge. A system or service has audit relevance when it initiates, authorises, processes, records, calculates, consolidates, reports or discloses information linked to a material transaction class, account balance or disclosure. The same principle covers system-generated reports used as audit evidence. A cyber weakness in a peripheral system might remain outside the financial statement audit scope. A weakness in identity infrastructure, ERP, payment file, payroll platform, consolidation tool or outsourced accounting service enters the risk assessment once material reporting reliance exists.

Prior integrative work treats cybersecurity as an event, impact and response problem across accounting functions [2–4]. The present article narrows the unit of analysis to a traceable relation between a governance condition, a control state and an external-audit consequence. The narrower unit permits explicit documentation of what changed in the audit plan and why.

2.2. Governance Deficiency and Control Deficiency

The distinction changes the causal language used in the framework. Governance conditions influence control design, operation and monitoring. Control state influences financial reporting only where a material dependency exists. Audit consequences then divide into misstatement risk and evidence-reliability risk. Compensating or corrective controls affect residual risk at every stage. The revised model therefore uses arrows as reasoning links, not deterministic claims.

An “excessive” security control requires separate analysis. An over-restrictive access rule might impede operations while still lowering unauthorised-access risk. A temporary manual control might compensate for a wider governance weakness. The audit file should record the control objective, control state, business and reporting effect and residual risk. Labelling every governance weakness as a failed cyber control would obscure these distinctions.

2.3. Crosswalk with Existing Frameworks and Standards

The crosswalk limits the novelty claim. COSO already defines internal-control principles. COBIT already structures information-and-technology governance. NIST already organises cyber outcomes. ITGC methods already guide testing of shared controls. The ISAs already govern audit judgement and evidence. The article contributes a connective mechanism across these sources. Its unit of novelty is the translation record, not any single component. Table 2 presents the detailed positioning against established control, security and audit sources.

Table 2. Positioning against established control, security and audit sources.

Source	Primary Purpose	Audit Relevance	Added Step in the Revised Model
COSO Internal Control-Integrated Framework [33]	Five components and seventeen principles for operations, reporting and compliance objectives.	Control environment, risk assessment, control activities, information and communication, monitoring.	Adds a cyber-specific route from governance evidence and control state to material processes, assertions and evidence reliability.
COBIT 2019 [34]	Forty governance and management objectives for enterprise information and technology.	Risk governance, security, change, operations, service providers, assurance and accountability.	Adds financial-statement accounts, assertions, audit evidence and engagement responses.
NIST CSF 2.0 [35]	Outcome taxonomy across Govern, Identify, Protect, Detect, Respond and Recover.	Cyber outcomes, organisational profiles and risk communication.	Adds financial reporting dependency, audit materiality, assertion mapping and audit-file consequences.
IT general control methods	Control families for access, program change, computer operations, development and related domains.	Operating effectiveness of shared technology controls supporting applications and reports.	Adds a governance entry point, dual audit consequences and a reassessment loop after compensating controls.
ISA 315 and ISA 330 [36]	Risk identification and assessment, then audit responses.	Likelihood and magnitude, relevant controls, information systems and further procedures.	Supplies the traceability object that the engagement team assesses under the standards.
ISA 402, ISA 500, ISA 540, ISA 560, ISA 570, ISA 620 and ISA 701 [36]	Service organisations, evidence, estimates, subsequent events, going concern, specialist work and key audit matters.	Evidence quality, outsourced systems, incident estimates, later events, continuity and specialist input.	Connects cyber facts to specific evidence sources, procedures and reporting decisions.

2.4. Analytic Propositions

P1. Cybersecurity governance enters external audit through a control state, a reporting or disclosure process or both. Organisation-level weakness alone does not establish a material assertion risk.

P2. Financial reporting dependency determines audit scope. Material accounts, disclosures, estimates, transaction classes and evidence sources provide the link.

P3. Misstatement risk and evidence-reliability risk are separate outcomes. Either outcome might arise alone or both might arise together.

P4. Compensating, detective and corrective controls alter residual risk. The route is conditional and reversible, not deterministic.

P5. Audit response follows process materiality, likelihood, magnitude, control state and evidence quality. The framework maps reasoning but does not assign numerical probability.

3. Method

3.1. Design and Review Scope

The study uses a structured integrative review and documentary analysis. An integrative design suits a question spanning accounting, auditing, corporate governance and information systems, where relevant work uses different theories, measures and units of analysis [1–4]. The review is structured because the search sources, dates, eligibility rules, coding fields and synthesis steps are reported. It is not presented as an exhaustive systematic review or meta-analysis.

The unit of analysis is an explicit relation among at least two of the following: cybersecurity governance, cyber controls or incidents, financial reporting, internal control, disclosure, external audit, audit evidence or organisational response. Technical computer-security papers enter only when they contain a direct reporting or audit link. The study does not pool effect sizes because the retained studies examine different outcomes, samples and methods.

3.2. Search Sources, Search Blocks and Date Limits

The search was completed on 16 July 2026. The publication window ran from 1 January 2000 to 15 July 2026. Google Scholar served as the discovery index. Publisher and journal search services were then used to verify records and locate final metadata across Elsevier/ScienceDirect, Wiley Online Library, Springer Nature, Emerald Insight, Sage Journals, the American Accounting Association and MIS Quarterly. DOI pages or publisher records confirmed titles, authors, journal details and publication status. Table 3 presents the review search protocol.

Table 3. Review search protocol.

Search Block	Terms and Use
Core cyber terms	“cybersecurity” OR “information security” OR “data breach” OR “cyber incident”
Audit and reporting terms	“external audit” OR “audit fee” OR “audit quality” OR “financial reporting” OR “internal control” OR “audit evidence”
Governance and disclosure terms	“board oversight” OR “audit committee” OR “cyber governance” OR disclosure
Control terms	“IT general controls” OR “access management” OR “change management” OR “backup and recovery” OR “service organisation”
Targeted combinations	Core cyber terms were combined with each audit, reporting, governance, disclosure and control block.

Reference lists from retained review papers and focal studies were checked for eligible journal articles. Later papers citing central audit and disclosure studies were also checked. Search work stopped when added searches returned records already retained or studies outside the defined reporting-and-audit boundary.

3.3. Eligibility and Selection

A record entered the academic set when it met all four rules: peer-reviewed journal publication, English language, publication inside the date window and an explicit organisational link among cyber governance or incidents and financial reporting, internal control,

disclosure, audit or post-incident response. The review excluded purely technical work on cryptography, network vulnerability or malware without a reporting link. It also excluded consumer-privacy studies without an organisational audit link, editorials, vendor papers, conference papers, working papers where a journal version existed, duplicates and records with unverified bibliographic data.

Screening used two passes. The first pass assessed title, abstract and source type. The second pass read the available article record and coded the relation to governance, disclosure, internal control, audit response, organisational response or review synthesis. The final analytic set contains 32 peer-reviewed journal articles. Four institutional sources form a separate professional set: COSO, ISACA, NIST and IAASB [33–36]. Two SEC filings form the application set [37,38]. No initial-hit total is reported because publisher searches and citation chaining produce overlapping records, and the study does not claim exhaustive database coverage.

3.4. Coding and Synthesis

Synthesis followed five stages. First, studies were grouped by evidence stream. Second, constructs were separated by organisational level. Third, reported links were mapped into control, reporting and audit categories. Fourth, the categories were compared with COSO, COBIT, NIST CSF and the ISAs. Fifth, the revised route was tested against two public filings and a boundary case. The resulting model is an analytic synthesis, not a statistical estimate. Table 4 presents the coding fields used in the integrative synthesis.

Table 4. Coding fields used in the integrative synthesis.

Coding Family	Recorded Content
Bibliographic and design fields	Year, journal, jurisdiction, sample, method and focal outcome.
Governance fields	Board or committee oversight, risk ownership, reporting line, policy, resources, third-party governance and remediation.
Control fields	Access, change, logging, operations, recovery, incident response, service provider and disclosure controls.
Reporting fields	Affected process, account, transaction class, estimate, disclosure, assertion and period.
Audit fields	Misstatement risk, evidence reliability, controls reliance, substantive work, specialist input, legal work and reporting.
Boundary fields	Compensating control, corrective action, no reporting dependency, residual risk and unresolved uncertainty.

3.5. Official Guidance and Public Filings

Non-academic material now enters through a controlled documentary set. Official sources were retained where they define governance, internal control, security outcomes or audit duties [33–36]. Public SEC filings were retained where they provide company-reported incident facts and financial effects [37,38]. Consultancy, software-vendor and insurance commentary remained excluded from the evidence base because authorship, commercial purpose and source methods vary. The separation protects source provenance while answering the review concern about omission of professional material.

Interviews were not added during revision. The research question asks how documented research and professional sources connect, rather than how practitioners perceive cyber-audit work. A credible interview study would need a sampling frame across audit firms and roles, ethics approval, interview protocols, saturation rules and access safeguards

for confidential engagement evidence. Section 7 specifies such work as the next empirical test rather than presenting an unplanned interview sample as validation.

3.6. Method Boundary: Mapping Rather than Probability Estimation

Risk includes likelihood and magnitude. The framework does not estimate either term. It identifies the object requiring assessment: the governance condition, control state, process dependency, account or disclosure, assertion and evidence source. Engagement teams then assess likelihood and magnitude from entity-specific evidence under ISA 315 and design responses under ISA 330 [36]. A numerical index without calibrated incident data, loss distributions and external validation would create unsupported precision.

4. Evidence Synthesis

4.1. Governance and Cybersecurity Disclosure

Review papers show a dispersed research base across accounting, information systems, management and computer security [1–4]. Disclosure work forms the most developed accounting stream. Studies document changes in risk-factor content, firm-specificity, readability, governance features and regulatory response [9–16]. The common finding is not uniform disclosure quality. Rather, cyber reporting reflects exposure, governance, incentives, regulation and prior incidents.

Board and committee studies link oversight attributes with cyber disclosure [5–8]. The audit relevance lies in the quality and route of information reaching those charged with governance. Board minutes, committee papers, incident escalation records and remediation reports provide evidence about risk identification and disclosure decisions. Strong disclosure alone does not prove strong control operation. Weak disclosure might indicate poor governance, reporting incentives or an incomplete disclosure process. The auditor needs corroboration.

Disclosure therefore serves two audit roles. First, it is reported information requiring evaluation for consistency with evidence elsewhere in the engagement. Second, it is a risk signal which directs inquiry towards systems, incidents, service providers, legal exposure and remediation. These roles differ. A well-written risk factor might remain generic. An incident-linked disclosure requires direct work on financial effects, legal correspondence, insurance, estimates and later events.

4.2. Incidents, Internal Control and Audit Response

Breach and internal-control studies connect cyber events with control weaknesses, management action, restatement risk, litigation and peer effects [17–24]. Shared technology creates the bridge. Identity services, program changes, interfaces, databases, operations and recovery support both operational processes and financial reporting. A security event in shared infrastructure therefore raises questions about relevant controls even where no accounting entry was directly manipulated.

Audit studies report higher audit fees after breaches or in the presence of riskier cyber disclosures [25–29]. Evidence on audit quality does not support a simple claim of lower quality after every event. Rosati, Gogolin and Lynn report patterns consistent with added audit effort after incidents [25]. The model should therefore represent audit response as an active mediator. A cyber event affects audit outcomes through changed risk assessment, evidence work, specialist use, procedures and review rather than through an automatic fall in audit quality.

Organisational-response studies add a further layer. Reputation, crisis response, leadership consequences and learning shape remediation [30–32]. Such work supports the reassessment loop in the revised figure. Incident response and recovery might reduce

residual risk, yet remediation evidence requires testing. Announced action and operating effectiveness are not equivalent.

4.3. Shared IT Dependencies and Audit-Evidence Reliability

IT control research shows how access and technology-control weaknesses affect management information and reporting processes [19–22]. The audit consequence reaches beyond client-side misstatement. System-generated reports, transaction populations, exception reports, logs and automated-control evidence might become less reliable where source systems or privileged access are weak.

Evidence reliability deserves separate assessment for three reasons. First, a complete and accurate population is a precondition for sampling and analytics. Second, control testing often relies on logs, tickets, reports and configurations produced by the same environment under review. Third, an incident might destroy or alter evidence without producing an identified misstatement. An audit plan focused only on account risk might therefore rely on weak evidence.

The separation changes procedure design. An auditor might retain the same assertion risk but abandon reliance on a system report. Alternative evidence might come from independent bank records, external confirmations, customer records, supplier evidence, forensic images, service-auditor reports or reconstructed data. The distinction also guides specialist involvement. A specialist might assess log integrity, system architecture, change history or data extraction while the auditor retains responsibility for audit judgement [36].

4.4. What the Literature Still Does Not Supply

The evidence streams supply strong pieces but no shared audit documentation unit. Governance papers end at oversight or disclosure. Control papers end at weakness or remediation. Audit-fee papers end at pricing. Incident papers end at business or market effects. Professional sources define duties and control domains. The missing step is a record linking one observed condition to one material reporting dependency, one or more assertions, an evidence-reliability conclusion, a response and a reassessment. Section 5 formalises this record.

5. Revised Cybersecurity-to-Audit Framework

5.1. A Conditional, Non-Deterministic Model

Figure 1 replaces the earlier linear chain. The revised route begins with a governance condition and then assesses control state. A decision point tests compensating or corrective controls. Financial reporting dependency follows only where residual weakness remains. Audit consequences divide into misstatement risk and evidence reliability. Audit response then feeds reassessment and remediation.

1. Governance condition. Record the observed organisation-level matter, its source and the governance process involved.
2. Control state. Identify relevant preventive, detective and corrective controls, then assess design, implementation and operation.
3. Compensation and correction. Determine whether other controls interrupt the route or reduce residual risk.
4. Financial reporting dependency. Identify material processes, accounts, disclosures, estimates, transaction classes and service providers.
5. Dual audit consequence. Assess assertion-level misstatement risk separately from evidence-reliability risk.
6. Audit response. Link each assessed risk to controls work, substantive procedures, external evidence, specialist input, legal work or reporting.

7. Reassessment. Update residual risk when new incident facts, remediation evidence, later events or control results arise.

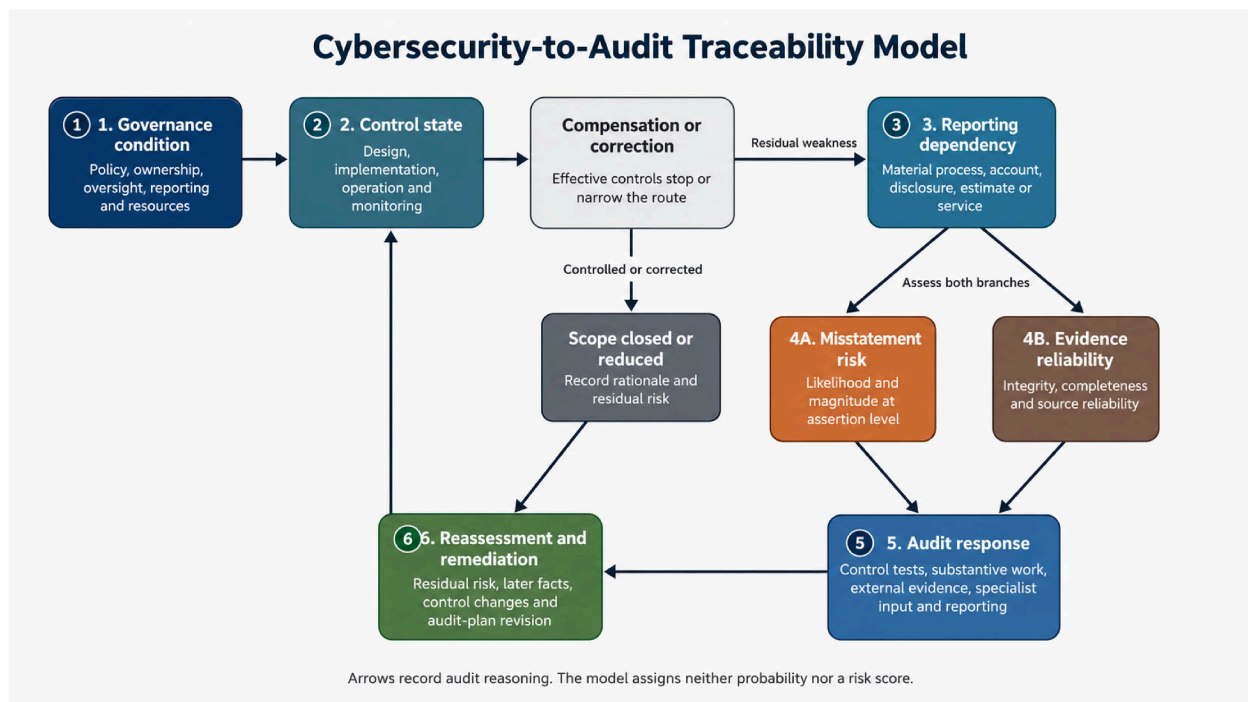


Figure 1. Cybersecurity-to-audit traceability model. Arrows represent audit reasoning links, not deterministic causation.

A governance weakness might stop at Step 2 where an effective control offsets the concern. A control deficiency might stop at Step 4 where the affected system has no material reporting dependency. A material incident might affect disclosure and estimates without weakening transaction processing. Evidence reliability might fail even where no identified misstatement exists. The route therefore supports several patterns rather than one causal chain.

5.2. File-Ready Traceability Protocol

Traceability is achieved when a reviewer is able to move in both directions. Forward tracing starts from the cyber fact and reaches the audit response. Reverse tracing starts from a procedure or conclusion and reaches the underlying condition, control state and reporting dependency. Missing links should lead to further inquiry or removal of unsupported audit work. Table 5 presents the traceability protocol for audit documentation.

Table 5. Traceability protocol for audit documentation.

Step	Required Record	Typical Evidence	Review Question
1. Source and condition	Document the event, governance concern or control finding and its evidence source.	Incident report, board paper, control test, service-provider notice, regulator letter.	What occurred or what weakness was observed?
2. Control state	Identify control objective, design, implementation, operation and monitoring.	Access review, change ticket, recovery test, logging configuration, incident plan.	Which control objective is affected, and what is the tested state?

Table 5. Cont.

Step	Required Record	Typical Evidence	Review Question
3. Compensation or correction	Record detective, manual, alternative or remediated controls.	Manual approval, independent reconciliation, restored backup, post-event review.	Does another control interrupt or reduce the route?
4. Reporting dependency	Map the system or service to material processes, accounts, disclosures or estimates.	System inventory, process map, data flow, report catalogue, service description.	Where does financial reporting rely on the affected item?
5. Assertion and evidence	Assess misstatement risk and evidence reliability separately.	Assertion matrix, population check, report logic, source validation.	Which assertions and evidence sources are exposed?
6. Response and reassessment	Link procedures, specialist work, reporting and later updates.	Audit programme, specialist scope, legal inquiry, disclosure checklist, review note.	What changed in the audit plan, and what residual risk remains?

5.3. Expanded Assertion-Based Mapping

Table 6 extends the earlier matrix in four ways. Accounts and disclosures are explicit. Evidence sources are explicit. Specialist involvement is conditional rather than automatic. Standard links show where established audit duties govern the response. The tables remain examples, not a universal programme. Engagement teams still tailor work to materiality, assessed risk, system design and available evidence.

Table 6. Cyber conditions, reporting dependencies, assertions and evidence risk. Audit procedures, evidence sources and specialist or standard links.

Condition	Processes, Accounts or Disclosures	Assertions	Evidence-Reliability Issue
Governance and reporting-line deficiency	Entity-wide risk assessment, incident escalation, disclosure process. Notes, provisions and going-concern analysis.	Completeness, valuation, presentation.	Management information might omit incidents or remediation. Board records might conflict with disclosures.
Privileged-access deficiency	General ledger, journals, payables, cash, revenue, payroll and master data.	Occurrence, accuracy, rights and obligations, classification.	User listings, activity logs and report populations might be altered or incomplete.
Change-management deficiency	ERP logic, billing, revenue rules, inventory costing, depreciation, tax, interfaces and consolidation.	Accuracy, completeness, valuation, cut-off.	Change logs, test records and system reports might not prove authorised deployment.
Logging and monitoring deficiency	Journal monitoring, interfaces, exception reporting, fraud detection and incident chronology.	Occurrence, completeness, accuracy, cut-off.	Audit trails might be incomplete, mutable or unavailable.

Table 6. Cont.

Condition	Processes, Accounts or Disclosures	Assertions	Evidence-Reliability Issue
Backup, recovery and resilience deficiency	Books and records, order processing, inventory, revenue cut-off and continuity forecasts.	Completeness, existence of records, cut-off, presentation.	Populations might be unavailable or reconstructed from uncertain sources.
Incident-response deficiency	Provisions, contingencies, legal claims, insurance, impairment, later events and disclosures.	Completeness, valuation, classification, presentation.	Incident facts, cost records and legal status might remain incomplete or inconsistent.
Third-party cyber-governance deficiency	Payroll, cloud ERP, payment processing, customer billing, data hosting and outsourced operations.	Occurrence, completeness, accuracy, presentation.	Service reports, incident notices and user-control evidence might be missing or stale.
Cyber-disclosure control deficiency	Risk factors, governance disclosure, incident disclosure, estimates and annual-report consistency.	Completeness, accuracy, presentation.	Public text might conflict with internal records, legal evidence or financial effects.
Condition	Core audit work	Evidence sources	Specialist and ISA links
Governance and reporting-line deficiency	Inspect board and committee reporting, risk ownership, escalation, disclosure decisions and remediation follow-up.	Board packs, committee minutes, risk registers, incident assessments, disclosure committee records.	Audit or cyber specialist where governance records contain technical matters. ISA 260, 265, 315, 701.
Privileged-access deficiency	Test access approval and recertification, segregation of duties, privileged activity, journal entries and master-file changes.	Identity records, role matrices, activity logs, journal data, supplier changes, bank confirmations.	IT audit specialist for access design and log extraction. ISA 240, 315, 330, 500, 620.
Change-management deficiency	Inspect tickets, approvals, testing, migration, emergency changes and developer access. Reperform key calculations or reconcile source to ledger.	Ticketing records, code migration logs, test scripts, configuration evidence, independent recalculation.	Application or data specialist where logic is technical. ISA 315, 330, 500, 540, 620.
Logging and monitoring deficiency	Test log coverage and retention, validate population completeness, compare independent timestamps and expand substantive work where needed.	Security logs, database records, external records, interface totals, forensic images.	Cyber or data specialist for log integrity. ISA 240, 315, 330, 500, 620.
Backup, recovery and resilience deficiency	Inspect recovery tests, restoration evidence, manual controls, data reconstruction and continuity forecasts.	Recovery logs, restored datasets, business-continuity plans, manual reconciliations, cash-flow forecasts.	Cyber specialist for recovery evidence. Valuation or restructuring support where continuity is affected. ISA 315, 330, 500, 570, 620.

Table 6. Cont.

Condition	Core audit work	Evidence sources	Specialist and ISA links
Incident-response deficiency	Inspect incident chronology, legal advice, regulator contact, costs, insurance, provisions, impairment and later events.	Incident reports, invoices, legal letters, insurance correspondence, board minutes, post-year-end evidence.	Legal, valuation or cyber specialist according to exposure. ISA 250, 500, 540, 560, 570, 620.
Third-party cyber-governance deficiency	Assess service scope, service-auditor report, user controls, incidents, contract duties, data ownership and alternative evidence.	SOC report, bridge letter, contracts, incident notice, management monitoring, external confirmations.	IT specialist where service controls are technical. ISA 402, 500, 620.
Cyber-disclosure control deficiency	Reconcile public text with internal evidence, financial effects, legal position, governance records and later events.	Draft filings, disclosure checklist, legal correspondence, board records, incident and cost data.	Legal or cyber input where wording depends on technical or regulatory facts. ISA 250, 500, 560, 701.

6. Worked Documentary Applications

6.1. The Clorox Company, Fiscal 2024 Form 10-K

The Clorox filing reports unauthorised activity identified in August 2023. Certain systems were taken offline. Business-continuity procedures included manual ordering and processing at a reduced operating rate. The disruption affected order processing, product availability, net sales and earnings. The company also reported interim controls during system downtime, recovery and forensic costs, insurance recoveries, governance reporting and later ERP implementation [37].

The model begins with an incident and governance evidence rather than an assumed governance failure. Relevant control states include incident response, system availability, manual processing, access containment, recovery and interim financial controls. The reporting dependencies include customer orders, revenue, receivables, inventory availability, cost records, insurance recovery and disclosure. Possible assertion work covers occurrence and completeness of sales, cut-off, valuation of incident costs and insurance and presentation of incident effects.

Evidence reliability requires separate attention. Automated order records were disrupted, while manual processes operated for a period. An audit team would need to establish population completeness across the transition, reconcile manual records with restored systems, inspect control design over interim processing and test system-generated reports after restoration. External evidence from customers, shipping records, cash receipts, insurers and service providers would reduce reliance on affected internal sources.

The filing also illustrates the correction loop. Interim controls and later restoration might reduce residual risk. Their existence does not settle operating effectiveness. Audit work should test the controls and reconcile incident facts with governance reports, financial statement notes and management conclusions about internal control. The application therefore shows why the revised route includes compensation, evidence reliability and reassessment.

6.2. MGM Resorts International, October 2023 Form 8-K

MGM reported a cybersecurity issue affecting certain US systems, system shutdowns, property disruption and restoration work. Management estimated an adverse September ef-

fect of about USD 100 million on Adjusted Property EBITDAR and less than USD 10 million in one-time costs. The filing stated no expected material annual effect on financial condition and results while also reporting unauthorised access to some customer information and uncertainty over full costs and effects [38].

The reporting dependencies differ from Clorox. Reservation and guest-facing systems connect with occupancy, gaming and hotel revenue, cash collection, customer obligations, loyalty activity and operational statistics. The incident also creates possible legal, notification, identity-protection, advisory, insurance and regulatory costs. Audit work should separate the non-GAAP performance estimate in the filing from financial-statement accounts and disclosures.

Assertion analysis would focus on completeness and cut-off of revenue during disruption, accuracy of system interfaces, completeness and valuation of incident costs, insurance recognition, legal contingencies and presentation. Evidence reliability work would examine booking, occupancy and transaction populations during shutdown and restoration. Independent payment, bank, guest and property records might support completeness where central systems were unavailable.

The filing also illustrates materiality discipline. A large operational estimate does not, on its own, establish a material financial-statement misstatement. The auditor assesses recognised amounts, disclosures, likelihood, magnitude and annual context. The framework therefore maps the affected objects while leaving the materiality conclusion to engagement evidence and the applicable reporting basis.

6.3. Cross-Case Application and Boundary Test

The applications support face validity and usability. Each filing permits a trace from reported incident facts to reporting objects and audit work. The boundary case shows the model does not pull every cyber event into detailed financial statement testing. None of the cases tests predictive accuracy, completeness across industries or audit effectiveness. Such tests require audit files, interviews, inspection material or larger case samples. Table 7 presents the worked applications and associated scope boundaries.

Table 7. Worked applications and a scope boundary.

Case	Observed Condition	Reporting Objects	Audit and Evidence Focus	Framework Outcome
Clorox	Order-processing disruption, manual procedures, interim controls, recovery costs and insurance.	Revenue, receivables, inventory, incident costs, insurance, disclosures.	Population completeness across manual and restored systems. Test interim controls and external evidence.	Strong direct financial reporting dependency.
MGM	Guest-system disruption, property effects, customer-data access, advisory and legal costs.	Revenue, cash, incident costs, contingencies, insurance and disclosures.	Booking and transaction completeness during shutdown and restoration. Separate non-GAAP estimate from accounts.	Direct dependency with materiality judged in annual context.
Boundary case	Contained phishing event in an isolated marketing tool. No personal data, legal duty, material process or audit evidence affected.	No material account, disclosure, estimate or evidence source.	Document inquiry and scope conclusion. No added account testing without other indicators.	Route stops at reporting-dependency assessment.

7. Discussion

7.1. Incremental Contribution

The revised contribution is narrower and more defensible than a claim of a new general cyber framework. Existing research and professional sources already contain the component concepts. The article adds a translation architecture across them. Three features distinguish the architecture.

First, organisational level is explicit. Governance deficiency and control deficiency no longer appear as interchangeable terms. The model records the governance condition, then tests the state of relevant controls. Second, financial reporting dependency operates as a scope gate. The gate prevents broad cyber concern from becoming unsupported audit work. Third, audit consequences divide into misstatement risk and evidence reliability. The split changes procedure design because an audit team might retain an assertion risk while rejecting an internal report as evidence.

A further contribution lies in reversibility. Corrective action, manual controls, independent reconciliations and restored systems might reduce residual risk. The model requires reassessment rather than assuming an uninterrupted chain. The design therefore answers the concern over policy weakness, risk-analysis weakness and control state. Different governance conditions enter through different evidence and might lead to different control conclusions.

7.2. Standards and Practice

The model sits inside, rather than beside, the ISAs. ISA 315 governs risk identification and assessment. ISA 330 governs responses. ISA 500 governs evidence. ISA 402 governs reliance on service organisations. ISA 540 covers estimates such as provisions and insurance. ISA 560 covers later events. ISA 570 covers continuity. ISA 620 governs use of an auditor's specialist. ISA 701 might affect key audit matter reporting in applicable engagements [36].

The same logic connects with COSO, COBIT and NIST [33–35]. COSO frames control components. COBIT frames governance and management objectives. NIST frames cyber outcomes. The proposed record moves from those constructs to accounts, assertions and evidence. It therefore avoids substituting a cyber framework for audit judgement.

Practical use begins during planning and continues after incidents or control findings. The team records system dependencies, aligns cyber findings with material processes, tests control state, evaluates evidence sources and revises procedures. Audit committee discussion becomes more specific because it identifies the affected process, assertion and response rather than asking whether cybersecurity was “covered”.

7.3. Materiality and Probability

The model does not turn qualitative mapping into risk measurement. Probability remains an engagement judgement based on incident facts, threat exposure, control state, prior errors, susceptibility to fraud and other evidence. Magnitude depends on affected accounts, transaction volumes, duration, legal exposure, disclosure needs and possible aggregation. The mapping identifies where those judgements belong.

Direct cash cost is one materiality input. Reporting dependency is another. A low-cost incident affecting a consolidation tool or a revenue population might require extensive work. A public event involving an isolated peripheral system might require limited financial statement work after disclosure and legal duties are cleared. Control materiality, financial materiality and disclosure materiality should therefore be considered separately, then assessed together under the reporting framework and auditing standards.

Qualitative categories such as low, medium and high are not included because labels without calibration differ across entities and audit firms. Later empirical work might

develop tested scales. The present framework deliberately preserves audit judgement and exposes the evidence behind it.

7.4. Limitations and Research Programme

1. The structured review is not an exhaustive census. Google Scholar and publisher services provided broad coverage, yet a database-replicated review across Scopus, Web of Science and specialist indexes might identify further studies.
2. The coding and synthesis are interpretive. A second independent coding team was not used. Later work should test inter-coder agreement and alternative construct boundaries.
3. The two public filings provide transparent worked application, not empirical validation. Public disclosures omit confidential audit evidence, detailed control tests and legal advice.
4. The framework does not estimate probability, expected loss, control effectiveness or audit quality. Tested measurement requires larger samples and outcome data.
5. Industry tailoring remains necessary. Banks, insurers, manufacturers, retailers and technology firms rely on different systems, services and regulatory duties.

The research programme follows from these limits. Multi-case studies should code incidents, controls, accounts, assertions and audit responses. Interviews with engagement partners, IT audit specialists, audit committee chairs, finance leaders and security leaders should examine decision paths and evidence disputes. Anonymised audit-file studies should test whether the traceability fields appear in practice and whether stronger records predict better review outcomes. Experimental work should test auditor judgements under alternative governance, control and evidence scenarios. Sector studies should tailor the matrix. Regulator and inspection cases should test external validity. Text and process-mining tools might support data extraction, yet human audit judgement remains responsible for scope and conclusions.

8. Conclusions

Cybersecurity enters external audit through a material financial reporting dependency or an audit-evidence dependency. Governance weakness alone does not establish a control failure. A control deficiency alone does not establish a material misstatement. Compensating and corrective controls might interrupt the route. Entity-specific likelihood, magnitude and evidence determine the audit conclusion.

The article supplies a structured link across governance, control, reporting and audit sources. The revised model records governance condition, control state, compensation or correction, financial reporting dependency, assertion-level misstatement risk, evidence reliability, audit response and reassessment. The dual treatment of misstatement and evidence reliability is central because compromised systems might weaken audit evidence even where no error has been identified.

The expanded tables identify accounts, disclosures, assertions, evidence sources, procedures, specialist roles and standard links. The Clorox and MGM applications show how public incident facts enter the model, while the boundary case limits scope. The framework remains qualitative and requires external testing. Its present value lies in disciplined, reviewable audit reasoning rather than numerical prediction.

Author Contributions: Conceptualisation, A.F. and S.T. Methodology, A.F. and S.T. Formal analysis, A.F. Investigation, A.F. and S.T. Writing, original draft preparation, A.F. Writing, review and editing, A.F. and S.T. All authors have read and agreed to the published version of the manuscript.

Funding: The research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new research data were created. The journal articles, institutional sources and public filings used in the review are identified in the reference list.

Acknowledgments: The authors acknowledge the academic resources and support provided by the University of Birmingham Dubai and Chulalongkorn University.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

Abbreviation	Meaning
COBIT	Control Objectives for Information and Related Technologies
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CSF	Cybersecurity Framework
ERP	Enterprise Resource Planning
IAASB	International Auditing and Assurance Standards Board
ICFR	Internal Control over Financial Reporting
ISA	International Standard on Auditing
ITGC	Information Technology General Controls
NIST	National Institute of Standards and Technology
PAM	Privileged Access Management
RMM	Risk of Material Misstatement
SOC	System and Organisation Controls report

References

1. Amani, F.; Magnan, M.; Moldovan, R. Cybersecurity Risks and Incidents Disclosure: A Literature Review. *Account. Perspect.* **2025**, *24*, 605–667. [\[CrossRef\]](#)
2. Walton, S.; Wheeler, P.R.; Zhang, Y.I.; Zhao, X.R. An Integrative Review and Analysis of Cybersecurity Research: Current State and Future Directions. *J. Inf. Syst.* **2021**, *35*, 155–186. [\[CrossRef\]](#)
3. Liu, C.; Babar, M.A. Corporate Cybersecurity Risk and Data Breaches: A Systematic Review of Empirical Research. *Aust. J. Manag.* **2026**, *51*, 62–92. [\[CrossRef\]](#)
4. Janvrin, D.J.; Wang, T. Linking Cybersecurity and Accounting: An Event, Impact, Response Framework. *Account. Horiz.* **2022**, *36*, 67–112. [\[CrossRef\]](#)
5. Zheng, G.; Xia, Z.; He, F.; Xiao, Z. The Audit Committee's IT Expertise and Its Impact on the Disclosure of Cybersecurity Risk. *Res. Int. Bus. Financ.* **2025**, *73*, 102542. [\[CrossRef\]](#)
6. Smaili, N.; Radu, C.; Khalili, A. Board Effectiveness and Cybersecurity Disclosure. *J. Manag. Gov.* **2023**, *27*, 1049–1071. [\[CrossRef\]](#)
7. Radu, C.; Smaili, N. Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure. *J. Bus. Ethics* **2022**, *177*, 351–374. [\[CrossRef\]](#)
8. Afroze, D.; Ghosh, R.; Dey, P.K. Cybersecurity Disclosure in the UK: The Role of Board Attributes and Female Director Critical Mass. *J. Enterp. Inf. Manag.* **2026**, *39*, 1309–1338. [\[CrossRef\]](#)
9. Gao, L.; Calderon, T.G. Cybersecurity Risk Governance and Companies' Cybersecurity Risk Disclosures in Their 10-K Filings. *J. Account. Public Policy* **2025**, *54*, 107376. [\[CrossRef\]](#)
10. Li, H.; No, W.G.; Wang, T. SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors. *Int. J. Account. Inf. Syst.* **2018**, *30*, 40–55. [\[CrossRef\]](#)
11. Gao, L.; Calderon, T.G.; Tang, F. Public Companies' Cybersecurity Risk Disclosures. *Int. J. Account. Inf. Syst.* **2020**, *38*, 100468. [\[CrossRef\]](#)
12. Calderon, T.G.; Gao, L. Changes in Corporate Cybersecurity Risk Disclosures after SEC Comment Letters. *J. Account. Public Policy* **2022**, *41*, 106993. [\[CrossRef\]](#)
13. Masoud, N.; Al-Utaibi, G. The Determinants of Cybersecurity Risk Disclosure in Firms' Financial Reporting: Empirical Evidence. *Res. Econ.* **2022**, *76*, 131–140. [\[CrossRef\]](#)
14. Singh, H. Voluntary Cybersecurity Risk Disclosures and Firms' Characteristics: The Moderating Role of the Knowledge-Intensive Industry. *Asian J. Account. Res.* **2025**, *10*, 168–185. [\[CrossRef\]](#)

15. López, F.A.; Jara-Sarrúa, L.; Morales-Parada, F.; Palos-Sánchez, P.R. Cybersecurity Disclosure in the Financial Sector: An Examination of the Influence of Incident Exposure, Governance Practices, and Regulatory Context. *Electron. Commer. Res.* **2025**, 1–35. [\[CrossRef\]](#)
16. Elsayed, D.H.; Ismail, T.H.; Ahmed, E.A. The Impact of Cybersecurity Disclosure on Banks' Performance: The Moderating Role of Corporate Governance in the MENA Region. *Future Bus. J.* **2024**, 10, 115. [\[CrossRef\]](#)
17. Zhou, F.; Huang, J. Cybersecurity Data Breaches and Internal Control. *Int. Rev. Financ. Anal.* **2024**, 93, 103174. [\[CrossRef\]](#)
18. Kelton, A.S.; Yang, Y.-W. Understanding Cybersecurity Breach Contagion Effects: The Role of the Loss Heuristic and Internal Controls. *Int. J. Account. Inf. Syst.* **2024**, 55, 100714. [\[CrossRef\]](#)
19. Li, C.; Peters, G.F.; Richardson, V.J.; Watson, M.W. The Consequences of Information Technology Control Weaknesses on Management Information Systems: The Case of Sarbanes-Oxley Internal Control Reports. *MIS Q.* **2012**, 36, 179–203. [\[CrossRef\]](#)
20. Steinbart, P.J.; Raschke, R.L.; Gal, G.; Dilla, W.N. The Relationship between Internal Audit and Information Security: An Exploratory Investigation. *Int. J. Account. Inf. Syst.* **2012**, 13, 228–243. [\[CrossRef\]](#)
21. Steinbart, P.J.; Raschke, R.L.; Gal, G.; Dilla, W.N. The Influence of a Good Relationship between the Internal Audit and Information Security Functions on Information Security Outcomes. *Account. Organ. Soc.* **2018**, 71, 15–29. [\[CrossRef\]](#)
22. Higgs, J.L.; Pinsker, R.E.; Smith, T.J.; Young, G.R. The Relationship between Board-Level Technology Committees and Reported Security Breaches. *J. Inf. Syst.* **2016**, 30, 79–98. [\[CrossRef\]](#)
23. Banker, R.D.; Feng, C.Q. The Impact of Information Security Breach Incidents on CIO Turnover. *J. Inf. Syst.* **2019**, 33, 309–329. [\[CrossRef\]](#)
24. Xu, H.; Guo, S.; Haislip, J.Z.; Pinsker, R.E. Earnings Management in Firms with Data Security Breaches. *J. Inf. Syst.* **2019**, 33, 267–284. [\[CrossRef\]](#)
25. Rosati, P.; Gogolin, F.; Lynn, T. Cyber-Security Incidents and Audit Quality. *Eur. Account. Rev.* **2022**, 31, 701–728. [\[CrossRef\]](#)
26. Yen, J.-C.; Lim, J.-H.; Wang, T.; Hsu, C. The Impact of Audit Firms' Characteristics on Audit Fees Following Information Security Breaches. *J. Account. Public Policy* **2018**, 37, 489–507. [\[CrossRef\]](#)
27. Smith, T.J.; Higgs, J.L.; Pinsker, R.E. Do Auditors Price Breach Risk in Their Audit Fees? *J. Inf. Syst.* **2019**, 33, 177–204. [\[CrossRef\]](#)
28. Calderon, T.G.; Gao, L. Cybersecurity Risks Disclosure and Implied Audit Risks: Evidence from Audit Fees. *Int. J. Audit.* **2021**, 25, 24–39. [\[CrossRef\]](#)
29. Bajpai, S.; Pathak, J.; Yadav, K. Cyber Risk, 10-K Report and Audit Fees. *Financ. Res. Lett.* **2026**, 91, 109496. [\[CrossRef\]](#)
30. Kamiya, S.; Kang, J.-K.; Kim, J.; Milidonis, A.; Stulz, R.M. Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms. *J. Financ. Econ.* **2021**, 139, 719–749. [\[CrossRef\]](#)
31. Gwebu, K.L.; Wang, J.; Wang, L. The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. *J. Manag. Inf. Syst.* **2018**, 35, 683–714. [\[CrossRef\]](#)
32. Nikkhah, H.R.; Grover, V. An Empirical Investigation of Company Response to Data Breaches. *MIS Q.* **2022**, 46, 2163–2196. [\[CrossRef\]](#)
33. Committee of Sponsoring Organizations of the Treadway Commission. *Internal Control-Integrated Framework*; COSO: Durham, NC, USA, 2013.
34. ISACA. *COBIT 2019 Framework: Governance and Management Objectives*; ISACA: Schaumburg, IL, USA, 2018.
35. National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*; NIST CSWP 29; NIST: Gaithersburg, MD, USA, 2024. [\[CrossRef\]](#)
36. International Auditing and Assurance Standards Board. *2025 Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements*; IAASB: New York, NY, USA, 2025; Volume 1.
37. The Clorox Company. Annual Report on Form 10-K for the Fiscal Year Ended 30 June 2024, Filed 8 August 2024. U.S. Securities and Exchange Commission. Available online: <https://www.sec.gov/Archives/edgar/data/21076/000002107624000030/clx-20240630.htm> (accessed on 8 January 2026).
38. MGM Resorts International. Current Report on Form 8-K, Filed 5 October 2023. U.S. Securities and Exchange Commission. Available online: <https://www.sec.gov/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm> (accessed on 15 July 2026).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.