International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 4, July – August 2026||

DOI:10.15662/IJRPETM.2026.0904008

From It Audit Findings to Cybersecurity Governance: A Risk-Based Remediation Framework for Critical Digital Infrastructure

Josephat Deogratius Katundabwile[1], **David Mbui Kamau** [2]

School of Engineering, The Catholic University of America, Washington, DC, United States of America[1]

katundabwile@cua.edu

The Catholic University of America, Washington, DC, United States of America[2]

kamaud@cua.edu

Publication History: Received: 10.06.2026; Revised: 27.07.2026; Accepted: 01.08. 2026; Published: 12.08.2026.

ABSTRACT: An IT audit finding does not reduce risk. Risk falls only when an organisation understands the finding, connects it to a critical system or business service, determines its risk level, assigns an accountable owner, implements a treatment, verifies that the treatment worked, formally addresses whatever risk remains, and reports progress to those charged with oversight. Evidence from the auditing and information systems literatures indicates that this chain breaks routinely, and that findings accumulate as open items rather than closing as reduced exposure. This article asks how organisations can convert audit findings into prioritised, accountable, measurable, and verified remediation, with particular attention to critical digital infrastructure, where an unremediated weakness affects service continuity for dependent sectors rather than the audited organisation alone. Using a structured narrative literature review of thirty peer-reviewed sources and seven authoritative frameworks, the review identifies four recurring failure modes: findings disconnected from business impact, ownership that is nominal rather than accountable, verification treated as administrative closure, and residual risk accepted informally. Drawing on enterprise risk management integration guidance, governance accountability models, and exploit-based prioritization research, the article proposes an eleven-stage risk-based remediation framework running from finding validation through continuous monitoring, together with eight measures spanning timeliness, ownership, verification quality, and business linkage. The framework is proposed rather than empirically validated, and no claim is made that it has produced measured improvement in any organisation.

KEYWORDS: IT audit; cybersecurity governance; risk remediation; enterprise risk management; critical digital infrastructure; three lines model

I. INTRODUCTION

Auditing detects. It does not repair. The distinction sounds obvious and is routinely lost in practice, because the artefacts an audit produces, namely findings, reports, and management responses, are so readily mistaken for the risk reduction they are meant to initiate. An organisation with a mature audit function and a long list of open findings is not a secure organisation. An organization knows where it is exposed.

The gap between identification and correction is well documented. Imdieke (2022) finds that whether a material weakness is remediated successfully depends heavily on the timing and character of management's remedial actions rather than on the identification of the weakness itself. Slapničar et al. (2022) show that the effectiveness of cybersecurity audit varies substantially with how audit interacts with the rest of the organisation, and Steinbart et al. (2018) demonstrate that the quality of the relationship between internal audit and information security shapes security outcomes directly. What these studies share is a conclusion that the value of audit is realised downstream of the audit, in a process the audit function does not control.

For critical digital infrastructure, the stakes of that downstream process are different in kind. Where an organisation supplies communications, computing, cloud, or data services on which other essential services depend, an unremediated weakness is not necessarily contained within the audited entity. It can propagate to dependants who had no visibility of the finding and no part in the decision to defer it (Pursiainen and Kytömaa, 2023). The question of who

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 4, July – August 2026||

DOI:10.15662/IJRPETM.2026.0904008

owns a finding, by when, and verified by whom therefore acquires a public dimension that ordinary internal control discussion does not capture.

This article addresses one question: how can organisations convert IT audit findings into prioritised, accountable, measurable, and verified cybersecurity risk remediation? Its objectives are to characterise the role of audit within cybersecurity governance, to identify why remediation fails, to examine how audit findings connect to enterprise risk management, to propose a risk-based remediation framework with defined accountability and measures, and to consider application in the United States regulatory environment. The contribution is integrative. The literature on audit effectiveness, governance accountability, vulnerability prioritisation, and enterprise risk integration each addresses part of the remediation chain, and none addresses the chain as a whole.

Section 2 reviews the literature and defines key terms. Section 3 sets out the theoretical framework and Section 4 the methodology. Section 5 presents the synthesis, the framework, and the measures. Section 6 discusses implications and limitations, Section 7 applies the framework to the United States context, and Section 8 concludes.

II. LITERATURE REVIEW

2.1 Key Concepts and Definitions

Critical digital infrastructure covers the communications, computing, cloud, data, and cybersecurity systems, and the supporting assets, on which essential services depend (Pursiainen and Kytömaa, 2023). **Cybersecurity governance** refers to the structures, decision rights, and accountability mechanisms through which an organisation directs and oversees its management of cyber risk, as distinct from the controls it operates (Savaş and Karataş, 2022). **Operational resilience** is the capacity to anticipate, absorb, adapt to, and recover from disruption while continuing to deliver critical services. **Engineering risk management** is the systematic identification, assessment, and treatment of technical failure modes affecting physical and logical assets. **Preventive maintenance** is maintenance performed at set intervals or against prescribed criteria to reduce the likelihood of failure or degradation. **Coordinated incident response** covers preparation, detection, analysis, containment, eradication, recovery, and post incident activity conducted across internal functions and external parties under a single command structure.

Three further terms carry specific meaning here. An **audit finding** is a documented gap between an observed condition and a defined criterion, whether that criterion derives from policy, regulation, or a control framework. **Remediation** is the set of actions taken to close that gap, and it is complete only when independently verified. **Residual risk** is the exposure remaining after treatment, which the organisation either reduces further or formally accepts at an authorised level (National Institute of Standards and Technology [NIST], 2025b).

2.2 The Role of IT Audit in Cybersecurity Governance

Internal audit occupies an unusual position in cybersecurity. It possesses neither the technical ownership of controls nor the executive authority to fund their improvement, yet it is the function most often charged with reporting on whether controls work. Steinbart et al. (2012) established early that the relationship between internal audit and information security is more consequential than either function's individual capability, and their later work found that a constructive relationship between the two is associated with better security outcomes, while an adversarial one degrades them (Steinbart et al., 2018).

Subsequent research has examined what makes cybersecurity audit effective. Slapničar et al. (2022) identify audit quality, auditor competence, and organisational responsiveness as determinants, and Vuko et al. (2024) approach the same question from a neo institutional perspective, arguing that legitimacy pressures shape audit effectiveness as much as by technical capability. Lois et al. (2021) document internal audit's procedural contribution to cybersecurity, and Calvin et al. (2025) characterise how internal audit activities engage with cybersecurity and information technology in practice.

Oversight above the audit function matters equally. Chen et al. (2022) find that audit committee information technology expertise is associated with data breach outcomes, and Lowry et al. (2025) provide field evidence that boards frequently lack the expertise to supervise cybersecurity effectively. Gale et al. (2022) examine governance of cybersecurity from the boardroom and identify persistent difficulty in translating technical reporting into oversight decisions. Taken together, these studies suggest that the remediation chain can fail at its top as readily as at its base: a finding correctly identified and correctly escalated can still stall if the receiving body cannot interpret it.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 4, July – August 2026||

DOI:10.15662/IJRPETM.2026.0904008

2.3 Why Remediation Fails

Four failure modes recur across the literature.

The first is disconnection from business impact. A finding expressed in control language, such as a missing configuration baseline or an incomplete access review, carries no inherent priority. Unless it is connected to an affected asset and thence to a business service, it competes for resources against operational work on unequal terms. NIST IR 8286A Revision 1 addresses this directly by requiring that cybersecurity risks be documented in registers that express them in terms of enterprise objectives (NIST, 2025a).

The second is nominal ownership. Assigning a finding to a department is not the same as assigning it to a person with authority over the resources needed to close it. Slapničar et al. (2023) develop a pathway model extending accountability beyond the conventional three lines, precisely because responsibility for cyber risk is distributed across roles whose formal authority does not match their practical influence.

The third is verification treated as administrative closure. Where the party that implemented a remediation also confirms its effectiveness, closure records the completion of an action rather than the reduction of a risk. Imdieke (2022) finds that failed remediation of material weaknesses is associated with the character of management's actions rather than their mere occurrence, and Patterson et al. (2023) find that organisational learning from security incidents is routinely blocked by incomplete records, a documentation problem that applies with equal force to remediation evidence.

The fourth is informal acceptance of residual risk. Findings that cannot be closed within available resources are frequently left open rather than formally accepted, which preserves the appearance of intent to remediate while producing none of the accountability that explicit acceptance would create. NIST IR 8286B treats risk response selection, including acceptance, as a decision requiring documented rationale and named authority (NIST, 2025d).

A fifth problem cuts across the others. Prioritisation by technical severity alone is a poor predictor of exploitation. Jacobs et al. (2020) demonstrate that remediation guided by exploit prediction outperforms severity-based approaches by a substantial margin, and the Exploit Prediction Scoring System developed from that work provides a probabilistic basis for prioritisation (Jacobs et al., 2021). Alqahtani and Almukaynizi (2026) extend this line by combining temporal threat intelligence with human input in a deployed patch prioritisation system. The implication for audit remediation is that the ordering of work should reflect likelihood of exploitation and consequence to the business, not the severity label attached at the point of discovery.

2.4 Connecting Audit Findings to Enterprise Risk Management

The integration of cybersecurity risk with enterprise risk management is the mechanism by which findings acquire comparable priority against other organisational risks. NIST IR 8286 Revision 1 sets out how cybersecurity risk management activities feed enterprise processes, aligning security decisions with strategic objectives and fiduciary responsibility (NIST, 2025b). Its supplements specify the stages: identification and estimation of risk and its documentation in cybersecurity risk registers (NIST, 2025a), prioritisation and response selection (NIST, 2025d), and aggregation for governance oversight (NIST, 2025c).

The register is the pivotal artefact. It converts a finding from an audit output into a managed risk with an owner, a treatment, a cost, and a status that can be aggregated upward. Without it, findings remain in audit tracking systems that management consults rather than operates. Pollmeier et al. (2023) illustrate the value of quantification in this context through a financial model for cyber risk developed in a banking case study, and Mojtahedi and Zhou (2024) show through analysis of information technology internal control material weaknesses that categories and trends in such weaknesses are traceable and industry dependent, which supports treating them as a managed risk class rather than as isolated defects.

Maturity models offer a complementary route. Büyüközkan and Güler (2025) review the cybersecurity maturity literature and propose a consolidated model, and COBIT provides governance and management objectives against which remediation processes themselves can be assessed (ISACA, 2018). Culot et al. (2021) caution, in reviewing the ISO/IEC 27001 literature, that certification and substantive security diverge, a caution that applies to remediation maturity as much as to management system certification.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 4, July – August 2026||

DOI:10.15662/IJRPETM.2026.0904008

2.5 Accountability Structures

The Three Lines Model assigns first line roles to those who own and manage risk, second line roles to those who provide expertise and monitoring, and third line roles to independent internal audit reporting to the governing body (Institute of Internal Auditors [IIA], 2020). Its application to cybersecurity is not straightforward. Valkenburg and Bongiovanni (2024) review the model's use in cybersecurity systematically and find inconsistent interpretation, particularly regarding where security operations sit. Héroux and Fortin (2024) examine how the three lines contribute to cybersecurity effectiveness in public firms and find the contribution contingent on how the lines interact rather than on their formal existence.

Two extensions are relevant. Slapničar et al. (2023) propose five lines of accountability, adding external assurance and the governing body as distinct accountable roles rather than recipients of reporting. Eulerich et al. (2025) demonstrate the use of process mining as an assurance tool within the three lines structure, which is significant for remediation because it offers evidence of whether a process was actually followed rather than whether it was documented.

III. THEORETICAL FRAMEWORK

Four positions provide the theoretical basis for the framework proposed in Section 5.

The first is enterprise risk integration. NIST IR 8286 Revision 1 holds that cybersecurity risk becomes governable when it is expressed, aggregated, and prioritised in the same terms as other enterprise risks, so that decisions about it are made against organisational objectives rather than in a technical enclave (NIST, 2025b). Applied here, this supplies the requirement that every finding be connected to an asset and a business service before it is prioritised.

The second is accountability theory as applied to governance. The Three Lines Model separates ownership, oversight, and independent assurance in order to prevent the party performing an activity from also attesting to it (Institute of Internal Auditors [IIA], 2020), and Slapničar et al. (2023) extend this separation to five roles. This supplies the framework's insistence that verification be independent of implementation, which is the structural answer to closure that records action rather than effect.

The third is probabilistic prioritisation. Jacobs et al. (2020, 2021) establish that likelihood of exploitation is empirically estimable and that prioritisation informed by it outperforms severity ranking. This supplies the framework's treatment of risk prioritisation as a judgement combining likelihood and business consequence rather than a reading of a severity field.

The fourth is organisational learning. Patterson et al. (2023) find that learning from security events depends on records adequate to support analysis and on mechanisms carrying findings into preventive practice. This supplies the framework's closing stages, in which recurrence data and verification failures return to the risk register rather than terminating in a closed ticket.

Together these yield a testable proposition: that remediation outcome improve where prioritisation reflects exploitation likelihood and service consequence, where verification is structurally independent of implementation, and where residual risk is accepted explicitly by a named authority rather than left open by default.

IV. METHODOLOGY

4.1 Design

This study employs a structured narrative literature review followed by conceptual framework development. A narrative approach was selected because the research question is integrative rather than effect estimating: it asks how several bodies of knowledge relate across a process chain, not whether a defined intervention produces a measured outcome. The review is structured in that source selection, thematic organisation, and synthesis followed the criteria below, but no claim is made to the exhaustiveness or reproducibility of a systematic review, and no meta analysis was performed.

4.2 Source Selection

The corpus comprises thirty peer reviewed sources and seven authoritative frameworks. Peer reviewed sources were selected across four thematic domains corresponding to the components of the research question: internal audit and cybersecurity audit effectiveness, governance and board oversight of cyber risk, vulnerability and remediation

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 4, July – August 2026||

DOI:10.15662/IJRPETM.2026.0904008

prioritisation, and critical infrastructure resilience. Selection prioritised publications from 2021 onward, with earlier work retained where foundational, as with Steinbart et al. (2012) on the audit and security relationship. Preference was given to systematic reviews where available.

The framework corpus comprises NIST IR 8286 Revision 1 and its supplements 8286A Revision 1, 8286B, and 8286C Revision 1; the NIST Cybersecurity Framework 2.0 (NIST, 2024); COBIT 2019 (ISACA, 2018); and the IIA Three Lines Model (IIA, 2020). These were included because remediation governance is shaped by authoritative guidance as much as by research literature. Version currency was checked rather than assumed: the 8286 series was substantially revised in December 2025, and the IIA Three Lines Model paper of July 2020, updated in September 2024, has since been superseded by a Statement of Position issued in July 2026 (Institute of Internal Auditors, 2026), so the 2020 paper is cited as the version underpinning the reviewed literature rather than as current guidance.

4.3 Synthesis and Framework Development

Sources were organised thematically rather than chronologically. Synthesis proceeded by mapping each domain onto the remediation chain and identifying which stages it addresses and which it leaves unspecified. Points of silence drove framework development, since the contribution sought was continuity across a process that the literature treats in fragments.

4.4 Use of Practitioner Insight

Practitioner perspective informed the framing of coordination and ownership problems in Sections 2.3 and 6.2. Two sources of applied experience are relevant: operations in a transmission network environment, and an applied cybersecurity risk assessment of public access library kiosks conducted as graduate coursework at The Catholic University of America. Both are used illustratively, in anonymised form, without organisational identifiers, configurations, credentials, incident records, or performance statistics. This material constitutes neither primary data nor empirical validation, and no analytical claim rests on it. In particular, the authors have not implemented the framework proposed here, or any control framework referenced in it, in any organisation, and no such implementation is claimed.

4.5 Methodological Limitations

Three limitations follow. Narrative selection carries a bias risk that systematic protocols reduce. The framework is conceptual and unmeasured, so its components rest on argument rather than outcome data. And a substantial portion of the empirical literature on audit and remediation originates in financial reporting contexts, where material weakness disclosure creates data availability that does not exist for cybersecurity findings generally, so its transferability to critical infrastructure operators is an assumption rather than a finding.

V. RESULTS

5.1 Synthesis of the Literature

The review identifies four literatures addressing parts of the remediation chain, developed largely independently.
Audit effectiveness research establishes that audit's contribution depends on its relationship with security functions and on organisational responsiveness (Steinbart et al., 2012, 2018; Slapničar et al., 2022; Vuko et al., 2024), but concentrates on the quality of the audit rather than on the fate of its findings. Governance and oversight research demonstrates that board and audit committee capability affects outcomes (Chen et al., 2022; Gale et al., 2022; Lowry et al., 2025) while treating the reporting that reaches the board as given rather than as an output whose construction is itself a governance problem. Prioritisation research provides an empirically grounded basis for ordering technical work (Jacobs et al., 2020, 2021; Alqahtani and Almukaynizi, 2026) but addresses vulnerabilities rather than audit findings, which include process and governance gaps for which no exploit probability exists. Enterprise risk integration guidance specifies how cybersecurity risk should be registered, prioritised, and aggregated (NIST, 2025a, 2025b, 2025c, 2025d) without addressing how findings enter that process from audit.

The integrative gap is therefore the chain itself. Each literature treats a segment as its endpoint: audit ends at the report, governance begins at the board pack, prioritisation begins at a scored vulnerability, and enterprise risk management begins at a registered risk. What is missing is a specification of the transitions between them and of who is accountable at each.

International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 4, July – August 2026||

DOI:10.15662/IJRPETM.2026.0904008

5.2 The Proposed Risk-Based Remediation Framework

The framework connects eleven stages into one governed sequence, presented in Figure 1. Each stage produces a defined output that becomes the input to the next, and the numbering is used throughout the discussion that follows.

Figure 1 *;* The eleven-stage risk-based remediation framework

Note. Developed by the authors. Stages proceed in sequence from 1 to 11. Two return paths operate: a failed independent verification at stage 9 returns the finding to stage 6 for a revised treatment decision, and continuous monitoring at stage 11 returns recurrence and effectiveness data to stage 4, reopening assessment where a closed finding recurs. Alternative text: a table of eleven numbered remediation stages grouped into four phases named establishing the finding, deciding, executing, and sustaining, with return paths from stage 9 to stage 6 and from stage 11 to stage 4.

The eleven stages group into four phases.

Establishing the finding. Validation confirms that the observed condition and the criterion are both correctly stated, which prevents remediation effort being spent on findings that dissolve under examination. Mapping to the affected asset and the critical service it supports converts a control gap into an exposure with consequence, and for critical digital infrastructure this mapping determines whether the consequence is internal or external to the organisation. Root cause analysis distinguishes the defect from its origin, since a finding closed at the symptom recurs.

Deciding. Likelihood and impact are assessed together, with likelihood informed where possible by exploitation evidence rather than severity alone (Jacobs et al., 2021), and impact expressed in terms of the service identified in the previous phase. Prioritisation orders findings across the portfolio rather than within an audit report. The treatment decision selects among reduction, transfer, avoidance, and acceptance, with rationale recorded (NIST, 2025d).

Executing. An accountable owner is named, meaning an individual with authority over the resources required, and a deadline is set proportionate to priority. Implementation proceeds. Independent verification then tests effectiveness, performed by a party other than the implementer, and testing the control's operation rather than the completion of the task. Where verification fails, the finding returns to the decision phase rather than closing.

Sustaining. Residual risk is accepted formally by a named authority at a level appropriate to its magnitude, with a review date, or is subjected to further treatment. Continuous monitoring tracks whether verified controls remain effective and whether closed findings recur, and feeds both back to the risk register.

The framework's distinguishing features are three. Business service mapping occurs before prioritisation rather than after, so that priority is derived from consequence rather than adjusted for it. Verification is structurally separated from

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 4, July – August 2026||

DOI:10.15662/IJRPETM.2026.0904008

implementation. In addition, residual risk has only two permitted states, formally accepted or under treatment, with the common third state of indefinitely open removed by design.

5.3 Proposed Measures

Measures should span the chain rather than concentrating at its end, since a programme can perform well on timeliness while failing on verification quality.

Measure	What it reveals
Overdue high risk findings	Volume of accepted exposure that no one has formally accepted
Average remediation time	Throughput, interpreted by priority band rather than in aggregate
Findings with named individual owners	Whether ownership is accountable or nominal
Recurrence rate	Whether root cause was addressed or the symptom was closed
Verification failure rate	Quality of implementation, and the value of independent testing
Formally accepted residual risks	Whether acceptance is an explicit decision or a default state
Control effectiveness improvement	Whether remediation changes control operation, not just status
Findings linked to business impact	Whether prioritisation has a consequence basis at all

Read in combination these expose specific pathologies. A short average remediation time with a high recurrence rate indicates speed achieved by closing symptoms. A low verification failure rate alongside rising recurrence suggests verification is confirming completion rather than testing effect. A high proportion of overdue high-risk findings with few formally accepted residual risks indicates that acceptance is happening in practice without happening in governance.

VI. DISCUSSION

6.1 Interpretation

The synthesis supports a specific reading of why remediation fails. The failure is not primarily analytical, since organisations generally know what is wrong once an audit has run, nor primarily technical, since most findings have known treatments. It is a failure of transition. Each function performs its own stage adequately and the handovers between them are unowned, which is why findings accumulate at the boundaries: between audit and management, between management and implementation, and between implementation and assurance.

This reframes what improvement requires. The framework does not ask audit to become responsible for remediation, which would compromise its independence, nor management to absorb assurance. It asks that the transitions be specified, that each have a named owner on both sides, and that the artefact carrying the finding across them, the risk register entry, be a single object rather than a set of parallel records maintained by different functions.

The proposition most open to challenge is the transfer of exploit based prioritisation from vulnerability management to audit findings. Jacobs et al. (2020, 2021) establish its value where exploitation probability is estimable, which is true of software vulnerabilities and false of governance findings such as an absent policy or an incomplete access recertification. The framework accommodates this by treating likelihood as evidence-informed where evidence exists and judgement-based where it does not, but the resulting hybrid has not been tested for consistency, and a programme that mixes probabilistic and judgemental likelihood estimates within one prioritised list may produce ordering that is defensible in each part and incoherent as a whole.

6.2 Implementation Considerations

Several conditions constrain adoption. Resource competition is the most common: remediation competes against delivery work, and its benefit appears as an absence, which is why the measures proposed above include leading indicators rather than outcomes alone. Ownership requires authority, and in organisations where technical staff hold responsibility without budget, named ownership becomes a formality; the framework's requirement that owners have resource authority is therefore a constraint on who may be named rather than an administrative field.

Independent verification requires capacity that smaller organisations may lack, and where a genuinely independent party is unavailable, separation within the same function combined with documentary evidence is a partial substitute rather than an equivalent. Legacy environments limit what verification can observe, a constraint familiar from operational technology settings where instrumentation predates current monitoring expectations (Miller et al., 2021).

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 4, July – August 2026||

DOI:10.15662/IJRPETM.2026.0904008

Third party dependencies complicate the chain further, since findings affecting supplier-delivered components require coordination that contracts alone do not produce (Wallis and Dorey, 2023).

Regulatory divergence adds a final complication. Where reporting obligations differ across jurisdictions, the same finding may carry different disclosure consequences depending on where the affected service operates, and Mentzelou et al. (2025) illustrate the compliance barriers this creates in the European context.

The following illustration shows how the framework's stages would apply. It is a constructed example, not a record of events, and is offered to make the sequence concrete rather than to evidence any outcome. Consider an assessment of publicly accessible information kiosks operated by a large institution, of the kind undertaken as graduate coursework. A review identifies that session data persists between users on shared terminals. Under stage one the finding is validated by confirming both the observed behaviour and the criterion it departs from. Stage two maps it to the affected asset and to the service the asset supports, which in this case is public information access, and this mapping is what establishes that the consequence falls on users rather than on the institution's own operations. Stage three distinguishes the defect from its origin, which may be a configuration setting or an absent policy governing shared-terminal builds. Stages four and five assess likelihood and impact and place the finding against others in the portfolio. Because no exploit probability applies to a configuration gap of this kind, likelihood is a judgement rather than an estimate, which is precisely the hybrid weakness identified in Section 6.1. Stage seven names an owner with authority over the terminal build rather than the department that operates the terminals. Stage nine tests whether session data actually clears, rather than confirming that a change request closed. The sequence illustrates the framework's central claim: the effort is concentrated at the transitions, not within the stages.

6.3 Limitations

The framework is proposed rather than validated. It rests on peer-reviewed literature, authoritative guidance, and anonymised practitioner perspectives, and no claim is made that it has produced measured improvement in any organisation. The measures are proposed on analytical grounds rather than calibrated against operational data, so thresholds would need local establishment. The empirical base is weighted toward financial reporting contexts, and the framework's applicability to operators whose findings are not subject to material weakness disclosure has not been examined.

VII. APPLICATION TO THE UNITED STATES CONTEXT

The United States presents a demanding case for remediation governance because its requirements arrive from several directions at once, each with a different definition of what must be fixed, disclosed, or attested.

7.1 Overlapping Obligations

Internal control over financial reporting under the Sarbanes-Oxley Act produces the most mature remediation discipline available to most organisations, since a material weakness must be disclosed and its remediation subsequently demonstrated. That discipline is where much of the empirical evidence cited in Section 2 originates (Imdieke, 2022; Mojtahedi and Zhou, 2024), and it is instructive that the strongest evidence on remediation effectiveness comes from the one domain where failure to remediate is publicly visible.

Cybersecurity disclosure operates separately. The Securities and Exchange Commission's 2023 rules require registrants to disclose material cybersecurity incidents on Form 8-K Item 1.05 within four business days of a materiality determination, and to describe risk management, strategy, and governance annually under Regulation S-K Item 106. Those rules remain in effect, though they are under active challenge: a rulemaking petition seeking rescission of Item 1.05 was filed in 2025, and in April 2026 several banking trade associations urged rescission or narrowing of both provisions in response to a Commission request for comment on Regulation S-K. Haapamäki and Sihvonen (2026) provide early evidence on what registrants actually disclose under these requirements, and Amani et al. (2025) review the broader disclosure literature.

Federal agencies and their suppliers operate under a third regime, in which the NIST IR 8286 series provides the mechanism for integrating cybersecurity risk into enterprise risk management and reporting it upward (NIST, 2025b). Critical infrastructure operators face a fourth. They may be subject to existing sector-specific reporting requirements, and are preparing for forthcoming obligations under the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which will become effective when the final rule of the Cybersecurity and Infrastructure Security Agency takes

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 4, July – August 2026||

DOI:10.15662/IJRPETM.2026.0904008

effect. The agency published a notice of proposed rulemaking in April 2024; as of the time of writing, the reporting requirements are not yet in force (Cybersecurity and Infrastructure Security Agency, n.d.).

7.2 Implications for the Framework

Three implications follow, and they are the reason the framework's early stages carry the weight they do.

Because obligations attach to consequence rather than to control category, the mapping of findings to affected assets and business services is what determines which regime applies. An organisation that prioritises findings by technical severity will discover its disclosure exposure late, since severity does not indicate materiality. Placing service mapping before prioritisation makes the regulatory determination a by-product of the risk process rather than a separate exercise conducted under time pressure.

Because the disclosure regime is unsettled, internal governance carries weight that regulation may or may not sustain. An organisation whose remediation discipline exists to satisfy Item 106 will find that discipline contingent on a rule under active reconsideration. One whose discipline rests on its own register, ownership, and verification structure is insulated from that uncertainty, and retains the evidence base that any successor requirement would demand.

Because the strongest remediation evidence comes from financial reporting, the transferable lesson is structural rather than substantive. What makes material weakness remediation comparatively effective is not the nature of the control but the combination of external visibility, a named accountable officer, and independent attestation. The framework proposed here reproduces the latter two internally for cybersecurity findings, which is the closest available substitute for the first.

VIII. CONCLUSION

This article has argued that audit findings reduce risk only when carried through a governed chain from validation to verified closure, and that the chain fails at its transitions rather than within its stages. The review found four literatures each treating a segment as its endpoint, leaving the handovers between audit, management, implementation, and assurance unspecified and unowned.

The proposed framework connects the eleven stages into one sequence with three distinguishing features: business service mapping precedes prioritisation, verification is structurally separate from implementation, and residual risk has no permitted indefinite state. Eight measures span the chain rather than concentrating on timeliness.

The contribution is integrative, and the framework is proposed rather than validated. Its central proposition, that remediation outcomes improve where prioritisation reflects exploitation likelihood and service consequence and where verification is independent of implementation, is testable and would benefit from testing. Three directions follow. Empirical evaluation in operating organisations would establish whether the transitions identified here are where remediation actually stalls. Work on likelihood estimation for governance findings, where exploit probability does not apply, would address the framework's weakest joint. And comparative study across disclosure regimes would clarify how external visibility shapes internal remediation discipline, which the financial reporting evidence suggests may be the strongest single determinant.

AUTHOR CONTRIBUTIONS

J. D. Katundabwile: conceptualisation; methodology; investigation; formal analysis; development of the risk-based remediation framework and measure set; provision of the applied telecommunications operations and cybersecurity risk assessment perspective informing Sections 2.3 and 6.2; writing of the original draft.

D. M. Kamau: validation; verification of literature and framework sources; writing, review, and editing; critical revision of the framework structure and the accountability analysis. Both authors have read and approved the final manuscript and accept responsibility for its content.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 4, July – August 2026||

DOI:10.15662/IJRPETM.2026.0904008

REFERENCES

1. Alqahtani, N., & Almukaynizi, M. (2026). VulnScore: A deployed system for patch prioritization combining human input and temporal threat intelligence. *International Journal of Information Security, 25*, Article 2. https://doi.org/10.1007/s10207-025-01164-3
2. Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity risks and incidents disclosure: A literature review. *Accounting Perspectives.* https://doi.org/10.1111/1911-3838.12411
3. Büyüközkan, G., & Güler, M. (2025). Cybersecurity maturity model: Systematic literature review and a proposed model. *Technological Forecasting and Social Change, 213*, 123996. https://doi.org/10.1016/j.techfore.2025.123996
4. Calvin, C., Cybersecurity and Infrastructure Security Agency. (n.d.). *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA): Frequently asked questions.* Retrieved August 19, 2026, from https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/circia/faqs
5. Chen, C., Hartmann, C. C., & Gottfried, A. (2022). The impact of audit committee IT expertise on data breaches. *Journal of Information Systems.* https://doi.org/10.2308/isys-2020-076
6. Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal, 33*(7), 76–105. https://doi.org/10.1108/tqm-09-2020-0202
7. Eulerich, M., & Holt, M. (2025). Characteristics of cybersecurity and IT involvement by the IA activity. *International Journal of Accounting Information Systems, 56*, 100726. https://doi.org/10.1016/j.accinf.2025.100726
8. Eulerich, M., Huang, Q., Pawlowski, J., & Vasarhelyi, M. A. (2025). Using process mining as an assurance tool in the three-lines-model. *International Journal of Accounting Information Systems, 56*, 100731. https://doi.org/10.1016/j.accinf.2025.100731
9. Gale, M., Bongiovanni, I., & Slapničar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security, 121*, 102840. https://doi.org/10.1016/j.cose.2022.102840
10. Haapamäki, E., & Sihvonen, J. (2026). Mandatory cybersecurity disclosure: Early evidence from 10-K reports. *International Journal of Accounting Information Systems, 57*, 100775. https://doi.org/10.1016/j.accinf.2026.100775
11. Héroux, S., & Fortin, A. (2024). How the three lines of defense can contribute to public firms' cybersecurity effectiveness. *International Journal of Disclosure and Governance, 22*(2), 377–396. https://doi.org/10.1057/s41310-024-00226-7
12. Imdieke, A. J. (2022). The role of timing and management's remediation actions in preventing failed remediation of material weaknesses in internal controls. *Contemporary Accounting Research, 39*(1), 157–198. https://doi.org/10.1111/1911-3846.12725
13. Institute of Internal Auditors. (2020). *The IIA's three lines model: An update of the three lines of defense.* The Institute of Internal Auditors.
14. Institute of Internal Auditors. (2026). *Statement of position: The three lines model.* The Institute of Internal Auditors.
15. ISACA. (2018). *COBIT 2019 framework: Introduction and methodology.* ISACA.
16. Jacobs, J., Romanosky, S., Adjerid, I., & Baker, W. (2020). Improving vulnerability remediation through better exploit prediction. *Journal of Cybersecurity, 6*(1). https://doi.org/10.1093/cybsec/tyaa015
17. Jacobs, J., Romanosky, S., Edwards, B., Adjerid, I., & Roytman, M. (2021). Exploit prediction scoring system (EPSS). *Digital Threats: Research and Practice, 2*(3), 1–17. https://doi.org/10.1145/3436242
18. Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: Audit role and procedural contribution. *International Journal of Managerial and Financial Accounting, 13*(1), 25. https://doi.org/10.1504/ijmfa.2021.116207
19. Lowry, M. R., Vance, A., & Vance, M. D. (2025). Inexpert supervision: Field evidence on boards' oversight of cybersecurity. *Management Science.* https://doi.org/10.1287/mnsc.2023.04147
20. Mentzelou, K., Chountalas, P. T., Kitsios, F. C., Magoutas, A. I., & Dasaklis, T. K. (2025). Identifying and modeling barriers to compliance with the NIS2 directive: A DEMATEL approach. *Journal of Cybersecurity and Privacy, 5*(4), 97. https://doi.org/10.3390/jcp5040097
21. Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. *International Journal of Critical Infrastructure Protection, 35*, 100464. https://doi.org/10.1016/j.ijcip.2021.100464
22. Mojtahedi, A., & Zhou, L. (2024). Information technology internal control material weaknesses in financial reporting: Categories, trends, associations, and industry effects. *International Journal of Accounting Information Systems, 53*, 100679. https://doi.org/10.1016/j.accinf.2024.100679

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 4, July – August 2026||

DOI:10.15662/IJRPETM.2026.0904008

23. National Institute of Standards and Technology. (2025d). *Prioritizing cybersecurity risk for enterprise risk management* (NIST Interagency Report 8286B, Update 1). https://doi.org/10.6028/NIST.IR.8286B-upd1
24. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). https://doi.org/10.6028/NIST.CSWP.29
25. National Institute of Standards and Technology. (2025a). *Identifying and estimating cybersecurity risk for enterprise risk management* (NIST Interagency Report 8286A, Rev. 1). https://doi.org/10.6028/NIST.IR.8286Ar1
26. National Institute of Standards and Technology. (2025b). *Integrating cybersecurity and enterprise risk management (ERM)* (NIST Interagency Report 8286, Rev. 1). https://doi.org/10.6028/NIST.IR.8286r1
27. National Institute of Standards and Technology. (2025c). *Staging cybersecurity risks for enterprise risk management and governance oversight* (NIST Interagency Report 8286C, Rev. 1). https://doi.org/10.6028/NIST.IR.8286Cr1
28. Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security, 132*, 103309. https://doi.org/10.1016/j.cose.2023.103309
29. Pollmeier, S., Bongiovanni, I., & Slapničar, S. (2023). Designing a financial quantification model for cyber risk: A case study in a bank. *Safety Science, 159*, 106022. https://doi.org/10.1016/j.ssci.2022.106022
30. Pursiainen, C., & Kytömaa, E. (2023). From European critical infrastructure protection to the resilience of European critical entities: What does it mean? *Sustainable and Resilient Infrastructure, 8*(sup1), 85–101. https://doi.org/10.1080/23789689.2022.2128562
31. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002).
32. Sathurshan, M., Saja, A., Thamboo, J., Haraguchi, M., & Navaratnam, S. (2022). Resilience of critical infrastructure systems: A systematic literature review of measurement frameworks. *Infrastructures, 7*(5), 67. https://doi.org/10.3390/infrastructures7050067
33. Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review, 3*(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4
34. Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. *International Journal of Accounting Information Systems, 51*, 100642. https://doi.org/10.1016/j.accinf.2023.100642
35. Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems, 44*, 100548. https://doi.org/10.1016/j.accinf.2021.100548
36. Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems, 13*(3), 228–243. https://doi.org/10.1016/j.accinf.2012.06.007
37. Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society, 71*, 15–29. https://doi.org/10.1016/j.aos.2018.04.005
38. U.S. Securities and Exchange Commission. (2023). *Cybersecurity risk management, strategy, governance, and incident disclosure* (Release Nos. 33-11216; 34-97989; File No. S7-09-22). https://www.sec.gov/rules/final/2023/33-11216.pdf
39. Valkenburg, B., & Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: A systematic literature review. *Computers & Security, 139*, 103708. https://doi.org/10.1016/j.cose.2024.103708
40. Vuko, T., Slapničar, S., Čular, M., & Drašček, M. (2024). Key drivers of cybersecurity audit effectiveness: A neo-institutional perspective. *International Journal of Auditing.* https://doi.org/10.1111/ijau.12365
41. Wallis, T., & Dorey, P. (2023). Implementing partnerships in energy supply chain cybersecurity resilience. *Energies, 16*(4), 1868. https://doi.org/10.3390/en16041868