International Journal of Scientific Interdisciplinary Research

**Volume:** 7; **Issue:** 1
**Pages:** 493–526

# Safeguarding Financial Records: A Cybersecurity-Driven Management Framework

**Mahmudul Hasan[1]; Sadia Zaman[2];**

[1]. *Master of Science in Management Information Systems, Lamar University, Texas, USA;*
*Email: mahmudulshojan601@gmail.com*

[2]. *Master of Science in Management Information Systems, Lamar University, Texas, USA;*
*Email: zaman.sadia1311@gmail.com*

*Doi: 10.63125/zch4s169*
***Received:*** *09 December 2025;* ***Revised:*** *19 January 2026;* ***Accepted:*** *21February 2026;* ***Published:*** *8 March 2026*

**Abstract**

*This study addressed the persistent problem that financial records stored and processed across cloud and enterprise platforms remain vulnerable to confidentiality, integrity, availability, and auditability failures because preventive controls are often implemented without equally strong monitoring, incident response readiness, and user compliance discipline. The purpose was to validate a cybersecurity-driven management framework that explains Financial Records Safeguarding Effectiveness (FRSE) within a quantitative, cross-sectional, case-based design using survey evidence from enterprise roles working with cloud and on-premises record workflows. Data were collected from 210 valid respondents drawn from finance and accounting (52.4%), audit and compliance (23.8%), and IT and security (23.8%), with 80.0% handling financial records weekly or more. Key variables included four independent constructs, Access Control and Authentication (ACA), Data Protection and Recovery Readiness (DPR), Awareness and Compliance Discipline (ACD, PMT-informed), and Monitoring and Incident Response Preparedness (MIRP), and the dependent construct FRSE, all measured on 5-point Likert scales. The analysis plan applied reliability testing (Cronbach's alpha), descriptive statistics, Pearson correlations, and multiple regression with multicollinearity checks. Findings showed moderate to high safeguarding maturity, with mean scores of ACA 3.82 (SD 0.64), DPR 3.71 (SD 0.66), ACD 3.58 (SD 0.70), MIRP 3.49 (SD 0.73), and FRSE 3.67 (SD 0.61); reliability was strong (a = 0.84–0.90 across constructs). FRSE correlated positively with all predictors, strongest with MIRP ($r = 0.71$, $p < .001$) and ACD ($r = 0.66$, $p < .001$). Regression results confirmed the integrated model was significant ($F(4,205) = 74.6$, $p < .001$) and explained substantial variance ($R^2 = 0.593$; Adjusted $R^2 = 0.585$), with MIRP the strongest predictor ($\beta = 0.36$, $p < .001$), followed by ACD ($\beta = 0.27$, $p < .001$), ACA ($\beta = 0.19$, $p = .002$), and DPR ($\beta = 0.12$, $p = .041$); VIF values (1.42–2.18) indicated no multicollinearity concern. A derived Threat Exposure Index averaged 0.266 (SD 0.122), with 18.6% low exposure, 62.4% moderate, and 19.0% high. Implications are that organizations should prioritize evidence-producing controls, especially monitoring and incident readiness, alongside PMT-aligned compliance strengthening, because these domains deliver the highest measurable gains in safeguarding effectiveness in cloud and enterprise financial record environments.*

**Keywords**

*Financial records safeguarding; cybersecurity management framework; monitoring and incident response; policy compliance discipline; cloud and enterprise governance;*

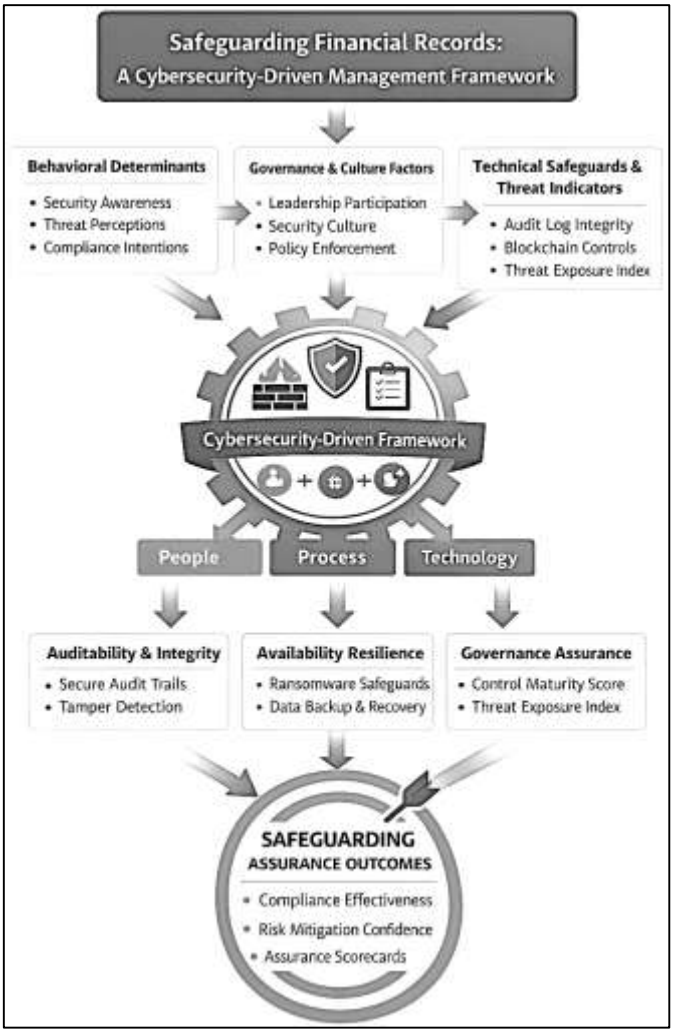
## INTRODUCTION

Financial records are the documentary evidence of economic activity—transactions, balances, authorizations, and audit trails—that enable reporting, compliance, and organizational accountability across jurisdictions and markets (AlHogail, 2015). In digital environments, "safeguarding" financial records can be defined as the coordinated set of governance, technical, and behavioral controls that preserve the confidentiality, integrity, availability, authenticity, and traceability of record content and metadata across the record life cycle (Alhogail & Alsabih, 2021). This definition aligns with how information security scholarship frames protection goals around access control, integrity preservation, and operational continuity, while recognizing that many record harms occur through routine organizational behaviors (e.g., policy noncompliance, insecure handling, weak logging) rather than rare technical failures (Herath & Rao, 2009a). Empirical research consistently positions policy compliance and security awareness as measurable determinants of whether controls actually protect organizational information assets, including data that supports accounting and financial reporting processes. In parallel, evidence from behavioral security shows that compliance is shaped by perceptions of threat severity and susceptibility, response efficacy, and self-efficacy—mechanisms frequently operationalized through structured survey instruments and modeled through statistical relationships suitable for quantitative research (Vishwanath et al., 2020). At the organizational level, the "security culture" construct provides a way to define shared norms, expectations, and routines that influence how people classify, store, access, transmit, and retain records in day-to-day work, turning abstract policy language into repeated practice (Bulgurcu et al., 2010). The international significance of safeguarding financial records is rooted in the cross-border interconnectedness of payment systems, capital markets, outsourced processing, and cloud-hosted accounting platforms; a single weakness in identity controls, audit logging, or governance can propagate into multi-entity reconciliation errors, unauthorized postings, or evidentiary disputes in audit and legal contexts. Secure logging and auditable evidence chains further reinforce the financial-records safeguarding objective because audit trails are themselves records that support accountability—yet they are attractive targets for tampering after intrusions, creating a direct link between cybersecurity engineering and record trustworthiness. Within this context, a cybersecurity-driven management framework is not merely a technical architecture; it is a socio-technical system in which controls, policies, culture, and measurable behaviors co-determine record protection outcomes (Vishwanath et al., 2011).

A cybersecurity-driven perspective treats financial records as both high-value assets and high-impact evidence, meaning the failure modes include not only unauthorized disclosure but also manipulated entries, incomplete audit trails, and degraded data quality that can impair decision-making and compliance (Cram et al., 2019). Research on security policy compliance provides empirical grounding that employees' rationality-based beliefs and awareness predict compliance intention—an important precursor to whether controls are executed correctly when interacting with sensitive records. Complementary work shows that persuasive security communications using fear appeals can influence security behavior, demonstrating that managerial interventions can be operationalized and evaluated rather than assumed effective (D'Arcy et al., 2009). Protection Motivation Theory (PMT)–based evidence in security contexts repeatedly ties perceived threat and coping appraisal to protective behaviors, supporting the use of PMT as a theoretical backbone for modeling safeguarding actions related to record handling, authentication practices, and secure workflow adherence. Beyond intention, policy compliance has been empirically studied as enacted behavior, with findings that rewards and sanctions do not operate uniformly across contexts, reinforcing the need to measure attitudes, self-efficacy, and organizational enabling conditions in a structured way (Gordon et al., 2010). Neutralization theory further supports the idea that individuals justify noncompliance through rationalizations, implying that safeguarding frameworks must account for "why exceptions become normal," especially in finance operations where deadline pressure and workload can encourage informal workarounds. A records safeguarding lens also includes integrity-centered mechanisms such as tamper-evident audit logging. Cryptographic secure logging work demonstrates practical approaches to forward-secure integrity and verifiable aggregation, which directly maps to protecting audit trails that substantiate financial record authenticity and chain-of-custody requirements. Infrastructure-level approaches using permissioned blockchains have been proposed and evaluated to

preserve log integrity and non-repudiation without relying on a single trusted party, an architectural pattern relevant to multi-department or multi-entity financial operations that require verifiable evidence (Ara, 2021; Herath & Rao, 2009b). On the threat side, ransomware research underscores that attacks can rapidly convert availability risk into operational and reporting risk, because encrypted or inaccessible accounting records disrupt reconciliation, payroll, billing, and statutory timelines (Ahmed & Hasan Or, 2021; Robel & Morshedul, 2021; Rosati et al., 2017). These findings collectively motivate an introduction that defines safeguarding financial records as a measurable, multi-layer construct—spanning people, process, and technology—capable of being examined through descriptive statistics, correlation structures, and regression relationships consistent with quantitative case-study analysis (Aditya & Robel, 2022; Istiaq & Nusrat, 2022; Rosati et al., 2018).

**Figure 1: Integrated Safeguarding Model Linking Behavioral, Governance, and Technical Controls**




In organizational settings, "management framework" refers to the structured alignment of governance, policies, controls, monitoring, and accountability mechanisms that translate security objectives into operational routines and measurable outcomes (Khaled & Hisham, 2022; Mehedi & Md, 2022). Empirical studies show that compliance behavior is influenced by top management participation and organizational culture, supporting a governance-first framing in which leadership involvement and cultural reinforcement are treated as measurable antecedents to safeguarding outcomes (Mainuddin & Chandra, 2022; Morshedul et al., 2022; Tandon et al., 2021). Research on information security culture provides validated constructs that can be adapted to financial-record contexts, including shared assumptions about responsibility, reporting, and control use—elements that strengthen or weaken the consistency of secure recordkeeping across teams and shifts. At the same time, evidence from accounting information systems research emphasizes that data quality risks have operational and

regulatory consequences; task-level control strategies that mitigate data quality risk are relevant to safeguarding because integrity failures in financial records often manifest as quality degradation, inconsistent master data, or unauthorized changes rather than overt "breach" events. From an economic and disclosure perspective, research in MIS Quarterly indicates that information security has observable market value implications when firms voluntarily disclose security-related information, which supports the broader organizational significance of safeguarding practices and the reputational sensitivity of financial data stewardship (Hsu et al., 2016; Nazmul & Begum, 2022; Shahinur & Sultan, 2022). Market-facing consequences are also reflected in empirical finance research examining how firms' breach-related communications and signals interact with investor response, reinforcing that safeguarding is evaluated externally through trust and risk perceptions, not only internally through control checklists (Begum & Kaniz, 2023; Rus, 2015; Binte & Hasan Or, 2022). In operational cybersecurity, auditable database practices represent a practical control domain where record safeguarding can be observed: database auditing methods and regulatory-aligned audit checklists offer concrete ways to structure monitoring of access, change events, and anomaly detection in data repositories that house ledger and subledger records. Secure, tamper-evident logging research further clarifies that log files are themselves targets for deletion or modification after compromise, and that local tamper-evident mechanisms can produce verifiable signals of manipulation—properties relevant when organizations must defend the authenticity of financial record histories (Ara & Onyinyechi, 2023; Islam & Aditya, 2023). Collectively, these studies support an introductory framing that treats safeguarding financial records as a governance-controlled, culture-enabled, and technically enforced system whose effectiveness is best assessed through measurable constructs—policy compliance, awareness, culture, auditability, and incident exposure—rather than informal assurances (Hu et al., 2012; Ahmed & Mehedi, 2023; Hasan Or et al., 2023).

This study is designed to achieve a set of clear, measurable objectives that directly align with the research title, the quantitative design, and the need for a cybersecurity-driven management framework for safeguarding financial records. The first objective is to identify and define the most critical cybersecurity management factors that influence how financial records are protected within a real organizational environment, focusing specifically on record-sensitive processes such as access authorization, transaction approval, record storage, audit logging, backup handling, retention enforcement, and secure disposal. The second objective is to measure the current safeguarding condition of financial records within the selected case-study context by using a structured Likert five-point scale survey instrument to capture respondent perceptions across the main safeguarding domains, including access control and authentication strength, data protection and recovery readiness, security awareness and policy compliance, and monitoring and incident response preparedness. The third objective is to statistically examine the strength and direction of relationships among these safeguarding constructs by applying descriptive statistics to summarize the data patterns and applying correlation analysis to determine how strongly each cybersecurity management factor is associated with overall safeguarding effectiveness. The fourth objective is to test the predictive power of the identified cybersecurity factors by employing multiple regression modeling to evaluate which constructs significantly explain variations in financial record safeguarding effectiveness, thereby validating the proposed framework using quantitative evidence. The fifth objective is to generate study-specific safeguarding performance outputs that translate statistical findings into interpretable control assurance artifacts, including a Threat Exposure Index that summarizes perceived vulnerabilities and operational weaknesses, a Control Maturity Profile that categorizes safeguarding practices into structured maturity levels, and a Safeguarding Assurance Scorecard that ranks the most influential safeguarding drivers and highlights priority improvement areas within the case-study environment. The sixth objective is to establish a practical and replicable measurement structure that can be used by organizations to assess their safeguarding readiness for financial records using consistent constructs, reliable indicators, and statistically supported relationships. Collectively, these objectives ensure that the study does not treat safeguarding as a generic cybersecurity goal, but instead measures it as an evidence-based management capability centered on the unique confidentiality, integrity, availability, and auditability requirements of financial records.

## LITERATURE REVIEW

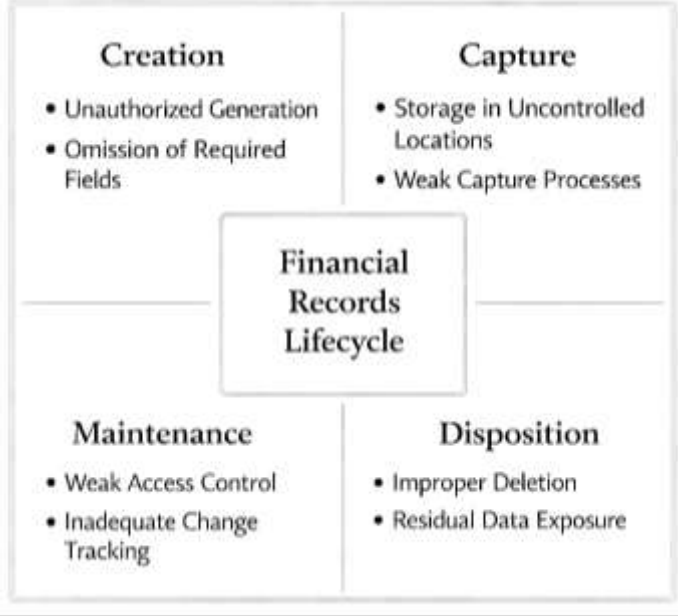
Safeguarding financial records is examined in the literature as a multi-layer problem that spans records management, accounting information systems, and cybersecurity governance, with particular emphasis on how confidentiality, integrity, availability, and auditability are sustained throughout the record life cycle. Financial records differ from general organizational data because they serve as both operational inputs and formal evidence for reporting, assurance, and accountability, which elevates the importance of trusted audit trails, controlled access, retention compliance, and recoverability in addition to preventing unauthorized disclosure. Prior scholarship situates this safeguarding challenge within socio-technical systems where policy, culture, and human behavior interact with technical controls such as identity and access management, encryption, logging, backup strategies, and monitoring. Empirical studies in information security policy compliance show that awareness, rationality-based beliefs, and perceived deterrence influence whether employees follow required controls in daily work, making compliance behavior a measurable contributor to protection outcomes. Behavioral security research also applies Protection Motivation Theory to explain how threat appraisal and coping appraisal shape protective actions, supporting theory-driven measurement of safeguarding behaviors relevant to financial record handling. At the organizational level, research on top management participation and information security culture highlights that leadership commitment and shared norms influence the consistency of policy adherence and the effectiveness of implemented controls, particularly in environments where time pressure and workflow complexity can encourage informal workarounds. Complementary technical literature addresses the integrity and non-repudiation dimensions of safeguarding by proposing cryptographic and infrastructure approaches for tamper-evident audit logging and verifiable evidence preservation, recognizing that logs and audit trails are critical to reconstructing events and defending record authenticity after incidents. Threat-focused research, including work on ransomware and data breaches, reinforces that disruptions to availability and trust in records can have direct operational and financial consequences, tying cybersecurity risk to continuity of finance functions. Collectively, the literature supports a structured approach to studying financial record safeguarding through integrated constructs that capture governance and culture influences, human compliance and awareness factors, and technical control maturity, enabling a cybersecurity-driven management framework to be empirically assessed using quantitative methods such as descriptive statistics, correlation analysis, and regression modeling.

### Financial Records Management and Record Lifecycle Risks

Financial records management sits within the broader discipline of records management, yet it carries distinctive characteristics because financial records function simultaneously as operational artifacts and as formal evidence for accountability, assurance, and dispute resolution. In organizational settings, financial records encompass transaction source documents, ledgers, subledgers, reconciliations, approvals, and the metadata that documents who created, accessed, or changed a record and when (Mainuddin & Chandra, 2023; Mehedi & Nahar, 2023). A lifecycle view treats these records as objects that must be created with sufficient context, captured into controlled systems, classified for retention, preserved in authentic form, and disposed of in a defensible manner. The literature emphasizes that the core quality of a record is not merely its informational content but its trustworthiness as evidence, which depends on maintaining reliability, authenticity, integrity, and usability over time (Mostafa, 2023; Chandra, 2023). In digital environments, these properties are challenged by system migrations, format obsolescence, distributed storage, and the ease with which content can be altered without visible traces. Managing electronic records requires explicit strategies and standards to preserve authenticity and reliability, because the evidentiary value of a record rests on being able to demonstrate its provenance and unbroken chain of control (Begum & Kaniz, 2024; Duranti, 2010; Khatun & Zakia, 2023). At the same time, records management work highlights that recordkeeping cannot be separated from organizational governance expectations, since financial records must support oversight, auditability, and legally defensible decision making. Records management has been framed as an essential component of information governance, positioning recordkeeping as a coordinated organizational function that links policy, responsibilities, and systems so that records can be trusted as accountable evidence across departments and stakeholder demands (Brooks, 2019; Khaled & Morshedul, 2024; Mehedi & Nahar, 2024). This perspective is salient for finance functions, where a

missing approval, incomplete reconciliation file, or altered timestamp can undermine audit assertions and confidence. Lifecycle risks include capture gaps, uncontrolled copies, inconsistent versions, and loss of context that prevents interpretation of why transactions occurred.

**Figure 2: Record Lifecycle Risk Framework for Financial Records**




Retention, appraisal, and disposition are especially consequential for financial records because they determine whether evidence persists long enough to meet legal, regulatory, and audit obligations, while also limiting accumulation of redundant or sensitive information that increases exposure (Md. Towhidul & Uddin, 2024; Robel & Morshedul, 2024). Within lifecycle models, appraisal establishes value categories and links them to retention rules, and disposal implements those rules through secure destruction or transfer to long-term preservation environments. Digital recordkeeping complicates these stages because records are fragmented across applications and communication channels, and because organizations often blur the boundary between transient working information and formal records (Albert, 2025; Zakia & Khatun, 2024). Email is a common example: finance approvals, exception handling, and supporting explanations frequently occur in messages that may never be captured into records systems, even when they contain essential context for later audits. Defensible deletion approaches for email show how deletion policies must be paired with systematic movement of important messages into corporate records systems if organizations are to preserve evidential needs while controlling storage growth (Ishtiaque & Rajib, 2025; Hasan, 2025; Lappin et al., 2019). For financial records, the same retention logic applies to files exported from accounting platforms, spreadsheet reconciliations, and attachments that evidence authorization or dispute resolution (Ashfaq & Ashraful, 2025; Robel, 2025). Appraisal decisions also have risk implications because they define which records remain available for oversight and which are removed from operational environments, and because disposal actions can introduce legal and reputational harm when they are not traceable, authorized, and consistently applied. Digital appraisal involves responsibility, norms, and value creation in a digitalized environment, reinforcing that appraisal is not only a technical sorting exercise but a governance activity that shapes accountability (Klett, 2019; Khaled, 2026; Murad, 2025). In finance contexts, appraisal criteria typically incorporate transaction significance, retention periods, audit sampling needs, and litigation hold requirements, and they must be applied to both content and metadata so that provenance and evidential links remain intact.

A lifecycle risk perspective also emphasizes that records management is interdependent with information security governance, because safeguarding requires coordinated controls across policy, technology, and roles rather than isolated procedures in either domain. As organizations digitize finance operations, recordkeeping is distributed across enterprise resource planning modules, shared

drives, content management platforms, collaboration tools, and outsourced services, creating multiple points where records can be copied, modified, or accessed outside approved workflows. Each stage of the lifecycle therefore introduces distinct security-relevant risks: creation risks include unauthorized generation of records or omission of required fields; capture risks include storage in uncontrolled locations; maintenance risks include weak access control and inadequate change tracking; preservation risks include loss of integrity during migration; and disposition risks include improper deletion or residual data exposure. Records management programs address these risks through policies for classification, retention schedules, version control, and authorized disposition, while information security programs address them through identity controls, encryption, monitoring, incident handling, and assurance practices. The relationships between records management and information security as organizational programs share overlapping objectives and dependencies, indicating that gaps at their interface can weaken overall protection (Xie, 2019). In financial record environments, interface gaps often appear when finance teams manage evidential files as "working documents" outside records systems, or when security teams monitor systems without visibility into which datasets constitute official financial records and which logs must be preserved for audit defensibility. A lifecycle framing clarifies the need for aligned ownership, clear definitions of record status, and consistent control enforcement across repositories so that evidence is not lost in routine operations. It also supports measurable assessment, because risks can be mapped to observable controls such as capture compliance, access review frequency, audit trail completeness, backup verification, and disposal authorization records. These measures operationalize financial record trust.

**Cyber Threat Landscape and Attack Vectors Targeting Financial Records**

Financial records are prime targets in the cybercrime ecosystem because they combine immediate monetization potential (fraud, extortion, resale) with strategic leverage (regulatory exposure, reputational harm, and operational disruption). In practical terms, "financial records" extend beyond ledger entries to include payment instructions, bank account identifiers, invoices, tax and audit files, payroll datasets, reconciliation reports, procurement documentation, and the underlying logs that evidence authorization and change history. A persistent feature of the threat landscape is that attackers rarely pursue a single record in isolation; they aim to compromise the *process* that produces, stores, approves, and audits records, because process compromise enables stealthy manipulation and repeat exploitation. The literature on phishing underscores that attackers exploit human trust and organizational workflows rather than attempting to defeat cryptography directly, making credential theft, session hijacking, and deception-driven approvals recurring pathways into record systems (Hong, 2012). This makes the "attack surface" of financial recordkeeping socio-technical: it includes email, identity and access management, approval routing, shared drives, enterprise resource planning modules, and third-party portals used for billing and reporting. At the system level, cybersecurity risk in finance is also characterized by interdependence and cascading effects, where an incident that begins as a localized compromise can become an enterprise-wide control failure due to shared infrastructure, shared credentials, or shared vendors (Ali et al., 2020). Consequently, safeguarding financial records requires treating threats as multi-stage campaigns that target both information assets and the governance structures meant to protect them.

A second dominant pattern in the contemporary threat landscape is the shift from "smash-and-grab" intrusions toward revenue-optimized, behavior-aware attacks that align with business rhythms and control routines. Ransomware illustrates this evolution by converting unauthorized access into coercive bargaining, where attackers exploit the operational value of record availability, the time pressure of closing cycles, and the dependency of compliance reporting on intact data (Laszka et al., 2017). From a records-management perspective, ransomware is not merely a confidentiality issue; it is an integrity-and-availability crisis that can suspend payroll, delay regulatory filings, and force manual workarounds that weaken segregation of duties. In parallel, large-scale data exposure incidents amplify identity theft and financial fraud risks, with documented links between breach events and downstream misuse of personal and transactional information, increasing the compliance burden on organizations that must notify affected parties and demonstrate diligence (Romanosky et al., 2011). These realities matter for record protection because disclosure requirements and audit scrutiny often focus on whether the organization can prove *what happened to the records*—who accessed them, whether they were altered,

and how quickly detection and containment occurred. Threat actors are therefore incentivized to tamper with logs, disable alerting, or alter approval traces to blur accountability. The most damaging outcomes frequently arise when compromised credentials allow attackers to operate "as a legitimate user," performing record-access and record-change actions that appear procedurally normal unless monitoring is designed around behavioral anomalies and control exceptions.

**Figure 3: Key Cyber Attack Pathways Against Financial Records**


Finally, the insider dimension remains structurally significant for financial record safeguarding because insiders (malicious or negligent) already possess contextual knowledge of systems, cycles, and control checkpoints. Evidence from financial-institution settings shows that insider threats are shaped by application characteristics and access patterns, meaning that certain business applications become predictably "attack-prone" due to their value, visibility, and accessibility within the organization (Wang et al., 2015). This insight is crucial for a cybersecurity-driven management framework because it suggests that record protection cannot be uniformly applied; it should be risk-weighted by process criticality and by how frequently an application is used to authorize, modify, or export financial data. When insiders or compromised insiders' accounts interact with records, harm can take the form of subtle ledger manipulation, invoice redirection, vendor master-file fraud, or the quiet deletion of supporting documentation that undermines audit trails. Such attacks often remain undetected because they exploit legitimate functions rather than triggering perimeter defenses. Therefore, the threat landscape for financial records is best understood as a convergence of (1) deception-led access (phishing and credential compromise), (2) coercion-led disruption (ransomware and operational extortion), (3) exposure-led fraud enablement (breaches feeding identity theft), and (4) access-led manipulation (insider and privileged misuse). This integrated view directly supports quantitative modeling in later sections by motivating measurable constructs such as exposure likelihood, control maturity, anomalous access frequency, and safeguarding assurance across record-centric workflows.

**Core Cybersecurity Controls for Safeguarding Financial Records**

Safeguarding financial records begins with treating accounting datasets, audit workpapers, payroll files, and transaction logs as high-value digital assets whose confidentiality must be engineered into storage and access pathways. In organizational practice, "data at rest" protections become decisive because many financial records reside for long periods inside database tables, document management repositories, backups, and cloud object storage, where unauthorized viewing can occur through compromised credentials or overly broad administrator access. Encryption at rest reduces the utility of stolen storage media or misconfigured storage permissions by ensuring that raw files and database exports remain unintelligible without the cryptographic keys. A practical implementation approach is to encrypt sensitive datasets prior to or at the moment they are placed into cloud storage, using

asymmetric or managed-key designs that maintain strong separation between infrastructure operators and the data owner's ability to decrypt (Sedayao et al., 2009). At the access layer, authentication strength and verification steps should align with the risk level of financial operations, because privileged access to ledgers, payment instructions, or financial statements can trigger fraud and regulatory exposure. Multi-factor authentication strengthens compliance-oriented interpretations of "appropriate security" by adding independent factors beyond passwords, supporting more defensible control narratives for financial-record access governance (Kennedy & Millard, 2016). In this study's context, encryption and stronger authentication are treated as foundational technical controls that enable subsequent measurement of safeguarding performance, because they directly shape how confidentiality and authorization are operationalized across record lifecycles, including retention, retrieval, archival storage, and controlled sharing.

Integrity and traceability requirements for financial records expand the safeguarding problem from confidentiality into verifiable accountability. Financial records are rarely static; they are adjusted, reclassified, corrected, and re-reported, which makes reliable monitoring essential for detecting anomalous access, suspicious modifications, and unauthorized extraction. Security monitoring is most effective when it prioritizes the protection of critical targets such as financial databases and reporting servers rather than focusing narrowly on identifying attacker origins, because organizational risk concentrates around the assets that generate regulatory reporting and financial decision support. Target-centric monitoring helps security teams design controls that focus on early detection of attacks against high-value nodes and on containment actions aligned with operational priorities (Shaikh & Kalutarage, 2016). Monitoring must also be paired with trustworthy evidence sources, particularly audit trails and database logs that can reconstruct "who did what, when, and how" across accounting systems and supporting repositories. In financial environments, tamper detection within databases is especially important because internal misuse and privileged misuse can alter records while attempting to erase traces. Database-forensic approaches emphasize structured evidence collection from redo logs, audit trails, timestamps, and archival logs to support reliable reconstruction and validation of record integrity following suspected manipulation (Tripathi & Meshram, 2012). Within the logic of this research, monitoring and tamper-evidence mechanisms support quantifiable safeguarding outcomes by enabling measurable indicators for threat exposure, control maturity, and assurance scoring at the case-study site.

**Figure 4: Core Cybersecurity Controls for Safeguarding Financial Records**


Operational resilience completes the safeguarding picture by ensuring that financial records remain available and verifiable during incidents, and that response actions preserve evidentiary value. Financial recordkeeping often supports statutory deadlines, audit cycles, and continuous operational

processes such as payroll and vendor settlement, which makes disruption itself a governance risk. Resilience therefore depends on incident response processes that integrate digital forensics into decision-making so that recovery actions do not erase crucial evidence needed for root-cause analysis, regulatory reporting, or legal defensibility. Incident response in many organizations tends to prioritize rapid restoration of services, while forensic work is treated as secondary; however, modern incident landscapes frequently involve multi-party infrastructures and cross-border threat activity, making forensic readiness and evidence preservation central to trustworthy control governance (Nikkel, 2014). In the context of safeguarding financial records, this means that backup restoration, containment, credential resets, and system hardening should be executed alongside controlled evidence capture, log preservation, and documentation of decision points. For this study, incident-response integration matters because it provides a measurable bridge between technical controls and managerial assurance: organizations can score higher on safeguarding credibility when they can demonstrate not only that controls exist, but that they function under stress conditions and produce auditable evidence. Accordingly, this subsection frames encryption and strong authentication, target-centric monitoring with tamper-evident logging, and forensics-integrated incident response as the technical–operational control backbone that the later empirical model can evaluate through constructs, correlation patterns, and regression-based predictors of safeguarding effectiveness.

**Protection Motivation Theory (PMT)**

Protection Motivation Theory (PMT) provides a behavioral-security lens for explaining why individuals adopt or neglect protective actions when handling sensitive organizational information. In the context of safeguarding financial records, PMT is valuable because it clarifies how employees and system users translate perceived cyber risk into daily compliance behaviors such as using strong authentication, avoiding insecure workarounds, protecting confidential exports, and following approved record-retention and sharing procedures. PMT conceptualizes protection as a motivated response shaped by two cognitive appraisals: threat appraisal and coping appraisal. Threat appraisal reflects how strongly a person believes a threat is serious and personally relevant, while coping appraisal reflects whether the person believes the recommended protective action is effective, feasible, and worth the effort. In information security research, PMT has been used to explain "knowing–doing gaps," where users understand protective requirements but still omit them in practice, demonstrating that awareness alone is not equivalent to motivated safeguarding behavior (Workman et al., 2008). The model has also been used to clarify how perceived vulnerability and perceived severity combine with efficacy beliefs to influence protective intentions and actions in technology-mediated environments, a logic that can be mapped to financial record workflows where routine access and routine handling create repeated decision points (Anderson & Agarwal, 2010). In addition, empirical work highlights that security practice is often linked to self-efficacy, meaning that users who believe they can successfully enact controls are more likely to behave securely, which is highly relevant for finance staff navigating complex systems and time-bound reporting cycles (Rhee et al., 2009). Within this study, PMT anchors the human-behavior side of safeguarding by explaining why policy compliance and secure record-handling behaviors vary across individuals and roles even when the same technical controls and formal policies exist.

Operationalizing PMT for a quantitative, cross-sectional case study requires converting its cognitive appraisals into measurable constructs aligned with financial record safeguarding behaviors. The literature supports measuring threat appraisal using indicators such as perceived severity (how damaging record compromise would be) and perceived vulnerability (how likely compromise is given the environment), and measuring coping appraisal using response efficacy (belief that controls work), self-efficacy (belief in one's ability to apply controls correctly), and response cost (perceived time/effort barriers). Studies show that these PMT components can be captured using structured Likert-scale items and modeled statistically as predictors of compliance or security practice behaviors (Boss et al., 2015). For the present research, PMT is implemented as the theoretical justification for the "awareness and compliance" domain within the safeguarding framework, and it also strengthens interpretation of differences across roles that interact with records in distinct ways (e.g., finance users creating and adjusting records, auditors reviewing evidence, IT/security maintaining access and logs). To support consistent measurement, PMT constructs can be summarized using composite indices that align with

standard survey scoring practices. For example, a simple threat appraisal score can be computed as: **TA = (PS + PV) / 2**, where PS is perceived severity and PV is perceived vulnerability, and a coping appraisal score can be computed as: **CA = (RE + SE − RC) / 3**, where RE is response efficacy, SE is self-efficacy, and RC is response cost (reverse-coded so higher values represent lower cost). The logic of these indices reflects how PMT-based studies conceptualize appraisals as weighted cognitive evaluations that translate into protective motivation and observable safeguarding behaviors (Vance et al., 2012). These PMT scores provide a theoretically grounded route for quantifying behavioral readiness to safeguard financial records within a bounded organizational case.

**Figure 5: Protection Motivation Theory (PMT) Framework for Financial Record Safeguarding**

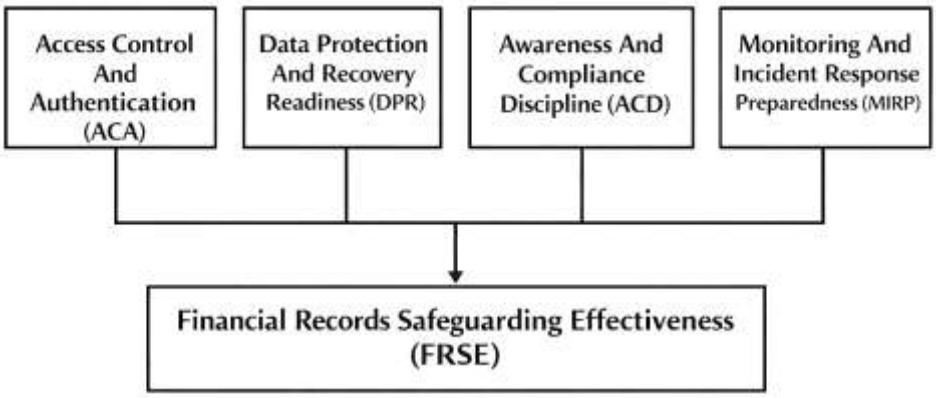

The study's cybersecurity-driven management framework integrates PMT with record-specific control domains so that safeguarding is assessed as a combined socio-technical capability rather than as a purely technical state. PMT is used to explain why users comply with access restrictions, follow secure sharing protocols, preserve record authenticity, and maintain trustworthy audit trails, while the technical domains of the framework represent the enabling control environment within which these behaviors occur. Empirical behavioral-security research indicates that motivational processes can be reinforced or weakened by habit and repeated practice, which matters in finance operations where closing routines and recurring transaction workflows can normalize either secure conduct or insecure shortcuts (Vance et al., 2012). Therefore, the framework treats safeguarding effectiveness as a measurable outcome that can be statistically predicted from a set of cybersecurity management factors, while PMT provides the interpretive logic for the human-driven variance embedded in those factors. The primary formula adopted for hypothesis testing and framework validation in this study is the multiple regression model, expressed as: $SFE = \beta_0 + \beta_1(AC) + \beta_2(DP) + \beta_3(AWC) + \beta_4(MIR) + \varepsilon$, where SFE is Financial Records Safeguarding Effectiveness, AC is Access Control and Authentication strength, DP is Data Protection and Recovery readiness, AWC is Awareness and Compliance (PMT-informed), MIR is Monitoring and Incident Response preparedness, $\beta$ terms are regression coefficients, and $\varepsilon$ is the error term. This equation is chosen because it aligns directly with the quantitative design, supports objective comparison of predictor strength through standardized coefficients, and can be extended to include PMT indices (TA and CA) as sub-dimensions or supporting predictors within the AWC domain when instrument design warrants such detail. Theoretical grounding through PMT strengthens the study's internal logic by ensuring that behavioral measures are not treated as generic attitudes, but as structured appraisals that connect perceived threat and coping capacity to safeguarding behavior in

financial record environments (Anderson & Agarwal, 2010).

**Cybersecurity-Driven Financial Records Safeguarding Model**

A conceptual framework for safeguarding financial records must convert the study's purpose into a structured cause–effect model that can be measured within a quantitative, cross-sectional, case-study setting. In this research, Financial Records Safeguarding Effectiveness (FRSE) is treated as the dependent construct representing the practical trustworthiness of financial records, meaning the extent to which records remain confidential, accurate, available, and auditable throughout their lifecycle (creation, approval, storage, retrieval, reporting, retention, and disposal). The model proposes that FRSE is driven by four control-oriented domains that are observable inside the case organization: (1) Access Control and Authentication (ACA), (2) Data Protection and Recovery Readiness (DPR), (3) Awareness and Compliance Discipline (ACD), and (4) Monitoring and Incident Response Preparedness (MIRP). This structure is consistent with governance-focused security literature that stresses alignment between organizational objectives, security policies, and continuous evaluation of controls as success factors for security governance outcomes (Chalmers et al., 2018). The framework also recognizes that financial record safeguarding is not evaluated only by "presence of controls," but by whether those controls produce reliable assurance evidence that supports reporting accountability and audit defensibility. Internal control research underscores that internal control quality has real consequences for stakeholders who rely on financial information, so the framework anchors safeguarding as an assurance-oriented capability rather than a purely technical feature (Lawson et al., 2017). In regulated financial reporting environments, implementation of recognized internal control frameworks (such as COSO 2013) influences how organizations operationalize control principles, document processes, and evaluate weaknesses, which strengthens the rationale for modeling safeguarding as a multi-domain management capability. Therefore, the conceptual framework used in this study connects cybersecurity controls and control governance to a measurable safeguarding outcome specific to financial record environments (Alghamdi et al., 2020).

**Figure 6: Conceptual Framework for Cybersecurity-Driven Financial Records Safeguarding Effectiveness (FRSE)**




To make the conceptual framework empirically testable, the study operationalizes each domain as a latent construct measured by multiple Likert-scale items and summarized into composite scores that can be used in correlation and regression analyses. The primary formula applied consistently across the study is the composite construct score for any domain $j$:

$$C_j = \frac{1}{m_j} \sum_{i=1}^{m_j} x_{ij}$$

where $x_{ij}$ is the respondent's Likert score on item $i$ for construct $j$, and $m_j$ is the number of items for that construct (with any barrier-type items reverse-coded so higher values always indicate stronger safeguarding). To translate the four domain scores into a single outcome-ready indicator that supports interpretation in the Results chapter (including scorecards and maturity profiles), the framework uses

an overall FRSE index computed as:

$$FRSE = \frac{ACA + DPR + ACD + MIRP}{4}$$

This equal-weight approach is selected because it preserves transparency in reporting and avoids arbitrary weighting unless the regression results justify differential influence through standardized beta coefficients. A complementary governance measurement logic is also embedded through maturity assessment thinking, where the organization's safeguarding capability can be interpreted as moving through staged levels based on the consistency and repeatability of practices, supporting the thesis's "control maturity profile" reporting. Together, these formulas provide a stable measurement backbone for descriptive statistics, correlation matrices, and regression modeling, ensuring that the conceptual framework is not only narrative but directly computable from survey responses (Rigon et al., 2014).

Conceptually, the framework also treats safeguarding outcomes as co-produced by finance staff, auditors, and IT/security stakeholders, because financial record protection depends on both system configuration and daily control execution. This means FRSE is expected to vary not only with the technical strength of controls but also with the degree to which business users participate in risk management activities, follow authorization workflows, and maintain evidence trails that auditors can rely on. Research on information systems security risk management shows that user participation can influence control selection, improve discovery of weaknesses, and shape perceptions of compliance-oriented security improvement, which supports modeling ACD as a key explanatory domain rather than a minor background factor (Spears & Barki, 2010). In practical finance operations, safeguarding failures often arise from workflow exceptions (urgent approvals, informal record transfers, "temporary" access elevation) that weaken auditability even when baseline controls exist. For this reason, the conceptual framework expects measurable linkages between ACD and MIRP: awareness and compliance discipline influences whether monitoring signals are meaningful and whether incident response preserves evidence and restores records with verifiable integrity (Lawson et al., 2017). The framework also supports the study's case-specific result artifacts by enabling two derived outputs from the same construct scores: a Threat Exposure Index (TEI) that summarizes perceived vulnerabilities (higher when FRSE sub-scores are lower), and a Safeguarding Assurance Scorecard that ranks domains by their predictive contribution in regression. In practice this alignment supports governance decisions and stronger audit defensibility.

**Gaps in Financial-Record Safeguarding Research**

Empirical cybersecurity literature consistently shows that security incidents translate into measurable organizational loss, which makes "safeguarding financial records" an outcomes-driven management problem rather than a purely technical compliance activity. Event-based evidence indicates that breach announcements can produce statistically significant negative market reactions, underscoring that stakeholders price cyber incidents as real economic shocks rather than as abstract IT issues (Goel & Shawky, 2009). This economic signal matters for financial records because accounting repositories, payment data, and reporting workpapers are often central to the information disclosed during incidents and to the remediation work that follows. Broader syntheses of event-study research reinforce the same theme: information security events are frequently associated with negative market responses across many contexts, suggesting that cyber incidents carry persistent valuation consequences (Spanos & Angelis, 2016). In organizational terms, these findings imply that record protection is tied to enterprise viability, audit continuity, and decision credibility—especially when incidents undermine reporting timelines, affect payroll or vendor settlement, or force manual record reconstruction. However, the empirical evidence base is often oriented around "breach occurrence" and "market reaction" rather than around the internal control pathways that determine whether records remain authentic, traceable, and recoverable. As a result, many studies establish that incidents are harmful but provide fewer directly measurable levers for managers to strengthen record safeguarding in day-to-day operations. This creates a gap between macro-level impact evidence and micro-level operational control evaluation. For a case-study organization, this gap translates into a practical need to move beyond incident counts and toward measurable control domains that can explain variance in safeguarding outcomes, such as access governance, monitoring strength, recovery readiness, and user

compliance discipline—so that safeguarding can be validated statistically rather than assumed from policy existence.

A second gap is the documented mismatch between perceived threats and implemented countermeasures, which is especially relevant to financial record environments where controls must align tightly with process risks such as authorization integrity, segregation of duties, and audit trail preservation. Cross-industry evidence shows that organizations may adopt countermeasures whose scope is not commensurate with the severity of threats perceived by decision makers, producing measurable "security gaps" between what is required and what is actually implemented (Yeh & Chang, 2007). In finance and accounting workflows, such misalignment can manifest as strong perimeter defenses alongside weak internal access segmentation, inconsistent approval traceability, or inadequate control over spreadsheet exports and reporting extracts. At the same time, empirical work on breach risk demonstrates that risk is contextual rather than uniform; it varies by organizational location, industry conditions, and breach history, meaning that organizations face differing baseline exposure even before considering their internal controls (Sen & Borle, 2015). These findings together indicate that safeguarding cannot rely on generic control checklists applied uniformly across all record processes. Instead, safeguarding must be modeled as a situational capability that accounts for organizational context and for where financial records sit in the operational value chain. Despite this, many organizational studies treat "security posture" as a single undifferentiated condition, while financial record safeguarding requires more granular distinctions among record creation, modification, approval, retention, backup, and auditability. This subsection therefore identifies a research need for a record-centered model that explicitly links context-sensitive exposure and control alignment to measurable safeguarding effectiveness within one organization.

**Figure 7: Empirical Research Gaps in Financial-Record Safeguarding Literature**

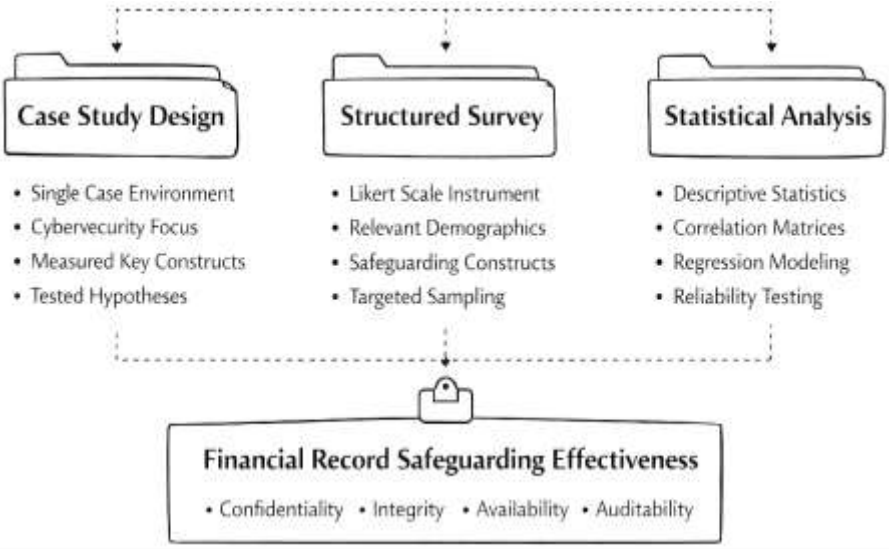

A third gap is that prior work often examines cyber incidents as externally visible events, while record safeguarding requires internal evidence of control performance, including integrity assurance and protection of high-value proprietary information embedded in financial and operational datasets. Research on breaches targeting trade secrets highlights that cyber theft is frequently directed at valuable proprietary information and that the disclosure environment around proprietary assets is associated with breach patterns, signaling that high-value information attracts targeted threats beyond generic data loss scenarios (Ettredge et al., 2018). Financial records share this "target value" characteristic because they encode pricing, margins, vendor structures, strategic spending, and transaction histories that can be exploited competitively or criminally. Consequently, safeguarding must be assessed through measurable assurance outputs that demonstrate control effectiveness for the case organization's record lifecycle, not only through generalized security maturity claims. To make this empirically testable, the study applies a consistent construct-scoring approach that converts Likert responses into domain indices and an overall safeguarding indicator used throughout descriptive, correlation, and regression analyses. The foundational measurement equation used across the study is

the composite scoring function: $C_j = \frac{1}{m_j}\sum_{i=1}^{m_j} x_{ij}$, where $C_j$is a construct score, $x_{ij}$is an item response, and $m_j$is the item count. The outcome indicator is computed as $FRSE = \frac{ACA+DPR+ACD+MIRP}{4}$, and a complementary exposure indicator can be expressed as $TEI = 1 - \frac{FRSE}{5}$when the Likert range is 1–5 (higher TEI indicates higher exposure). These formulas operationalize record safeguarding so that the study can evaluate which control domains most strongly explain safeguarding effectiveness and how the case organization's results translate into defensible, auditable assurance evidence, consistent with the economic significance documented in breach-impact studies.

**METHODOLOGY**

This study has adopted a quantitative, cross-sectional, case-study–based methodology to examine how a cybersecurity-driven management framework has influenced the safeguarding of financial records within an organizational context. The research design has been selected to enable systematic measurement of key safeguarding constructs and to support hypothesis testing through descriptive statistics, correlation analysis, and regression modeling. A single bounded case environment has been used to ensure that financial record processes, control structures, and governance routines have been examined within their real operational setting, where record creation, approval, storage, retrieval, reporting, retention, and disposal activities have been performed under established organizational policies. The study has treated financial record safeguarding effectiveness as the primary dependent construct, reflecting the degree to which confidentiality, integrity, availability, and auditability have been maintained across the record lifecycle. Core independent constructs have been defined to represent the main cybersecurity management domains that have shaped record protection, including access control and authentication strength, data protection and recovery readiness, awareness and compliance discipline, and monitoring and incident response preparedness.

**Figure 8: Research Methodology**




Data have been collected using a structured survey instrument that has been developed around a five-point Likert scale to capture respondent perceptions and experiences related to these safeguarding domains. The instrument has been organized into sections that have measured demographic attributes relevant to records interaction, followed by multi-item measures for each construct so that composite scores have been computed for statistical analysis. The target population has included organizational roles that have directly interacted with financial records or have supported financial record systems and controls, such as finance and accounting personnel, internal audit and compliance staff, and IT or security stakeholders. A sampling strategy has been applied to ensure representation across these groups within the case context, and ethical safeguards have been maintained through informed consent procedures, anonymity protections, and secure handling of collected responses.

To ensure rigor, the study has evaluated measurement reliability using internal consistency testing and has summarized construct patterns using descriptive statistics. Relationships among variables have been assessed through correlation matrices, and predictive effects have been tested through multiple regression modeling to determine which cybersecurity domains have significantly explained variations in safeguarding effectiveness. Statistical analysis software has been used to manage coding, computation, and model estimation, and the methodological structure has been aligned with the research questions, hypotheses, and conceptual framework established for this research.

**Research Design**

This study has employed a quantitative, cross-sectional, case-study–based research design to examine the safeguarding of financial records through a cybersecurity-driven management framework. The quantitative approach has been used to transform perceptions and control practices into measurable constructs using a structured Likert five-point scale instrument. A cross-sectional time frame has been selected so that data have been captured at one point in time, allowing the study to describe the current safeguarding condition and test relationships among key variables without requiring repeated measurement cycles. The case-study orientation has been adopted to ensure that safeguarding practices have been assessed within a real organizational setting where financial records have been created, accessed, stored, retained, and audited under existing governance procedures. This design has supported hypothesis testing through descriptive statistics, correlation analysis, and multiple regression modeling, enabling the study to validate its conceptual framework empirically.

**Case Study Context**

The study has been conducted within a bounded organizational case environment where financial records have been managed through integrated digital systems and formal governance processes. The case context has been selected because it has represented routine record-sensitive workflows such as transaction authorization, ledger posting, reconciliation, reporting, and retention scheduling. The organizational setting has included both business and technical stakeholders who have interacted with financial records directly or have maintained the systems that store and protect them. Record repositories have included accounting platforms or ERP modules, shared document repositories, and backup systems used to preserve evidence and continuity. The case has provided an appropriate environment for examining how cybersecurity controls have been embedded into financial record handling, including access restrictions, authentication practices, encryption, audit logging, monitoring, and incident response routines. This bounded context has enabled realistic measurement of safeguarding effectiveness and has supported interpretation of results through record-specific governance requirements.

**Population and Unit of Analysis**

The population for this study has consisted of organizational participants who have had direct responsibilities for creating, handling, reviewing, safeguarding, or supporting financial records and the systems that contain them. Respondents have included finance and accounting personnel responsible for transaction processing and reporting, internal audit and compliance staff responsible for assurance and governance, and IT or information security staff responsible for access provisioning, monitoring, backup administration, and incident readiness. The unit of analysis has been the individual respondent within the organizational case, because safeguarding behaviors, control adherence, and perceived control effectiveness have been expressed through individual actions and experiences within their role. This unit of analysis has supported the use of survey-based measurement, where individual perceptions have been aggregated into construct scores representing access control strength, data protection readiness, awareness and compliance discipline, and monitoring and incident response preparedness. This approach has allowed statistical testing of relationships between these constructs and overall safeguarding effectiveness.

**Sampling Strategy**

A structured sampling strategy has been applied to ensure that the study has captured responses from participants whose roles have reflected the key touchpoints of financial record safeguarding. The sampling approach has been designed to include stakeholders across finance operations, audit and compliance functions, and IT or security functions so that the dataset has represented both record creators and record protectors. A purposive method has been used to prioritize respondents who have

handled financial records, approved transactions, accessed reporting repositories, managed retention artifacts, or administered record-related systems and controls. Where organizational structure has allowed, stratification has been used to distribute participation across departments and job categories, reducing the risk that results have been driven by a single function's perspective. Inclusion criteria have required routine exposure to financial record workflows or safeguarding controls, ensuring relevance of responses. This strategy has strengthened the credibility of construct measures and has supported regression analysis by improving variability across predictors.

**Data Collection Procedure**

Data collection has been carried out using a structured questionnaire that has been distributed to eligible participants within the case organization through approved communication channels. Informed consent information has been provided at the beginning of the instrument, and anonymity protections have been maintained by avoiding the collection of direct personal identifiers. Participants have been informed about the study purpose, voluntary participation, and data confidentiality, and responses have been collected only after consent has been indicated. The survey has been administered within a defined time window so that responses have represented a consistent cross-sectional snapshot of safeguarding practices and perceptions. Completed responses have been exported into an analysis-ready dataset, and preliminary data screening has been performed to identify incomplete submissions, out-of-range values, and response patterns that have indicated low engagement. Data have been stored securely and have been accessed only for research purposes. These procedures have supported ethical integrity and have ensured that collected data have been suitable for quantitative analysis.

**Instrument Design**

The survey instrument has been designed to measure the main constructs of the cybersecurity-driven financial records safeguarding framework using multi-item Likert five-point scales. Items have been structured to capture practical safeguarding behaviors and control conditions relevant to financial records, including access control enforcement, authentication rigor, data encryption and secure storage practices, backup and recovery readiness, staff awareness and policy compliance discipline, monitoring quality, audit trail completeness, and incident response preparedness. The instrument has been divided into sections that have first captured demographic and role-related attributes, followed by construct-specific items that have represented each independent variable domain and the dependent safeguarding effectiveness domain. Item wording has been kept clear and role-appropriate so that finance users, auditors, and technical staff have been able to respond consistently based on their experience. Reverse-coded items have been included where necessary to reduce acquiescence bias. Composite construct scores have been computed using averaged item responses to support correlation and regression modeling.

**Pilot Testing**

Pilot testing has been conducted to confirm that the instrument has been understandable, role-appropriate, and capable of producing reliable measurements prior to full deployment. A small group of participants similar to the target population has been invited to complete the draft questionnaire so that item clarity, response time, and interpretation consistency have been evaluated. Feedback has been collected regarding ambiguous wording, overlapping items, and missing safeguarding dimensions related to financial record workflows. Based on pilot feedback, the instrument has been refined by rephrasing items with technical jargon, improving alignment between questions and construct definitions, and adjusting item order to improve flow and reduce respondent fatigue. Preliminary reliability checks have been performed on pilot responses to identify weak items and assess internal consistency trends. Items with low contribution to construct coherence have been modified or removed, and the final instrument has been confirmed to reflect the conceptual framework and theoretical grounding of the study. Pilot testing has strengthened measurement quality and has reduced risk of systematic response error.

**Validity and Reliability**

Validity and reliability procedures have been applied to ensure that the study's constructs have measured what they have been intended to measure and that results have been consistent. Content validity has been addressed by aligning survey items with established definitions of cybersecurity controls, financial record safeguarding requirements, and the theoretical and conceptual frameworks

adopted in the study. Expert review has been used to confirm that the instrument has covered essential safeguarding dimensions, including confidentiality, integrity, availability, and auditability. Construct validity has been supported by grouping items under clearly defined domains and by ensuring that item statements have reflected observable practices rather than abstract opinions. Reliability has been evaluated using internal consistency testing, where Cronbach's alpha has been computed for each construct to assess scale stability. Where alpha values have indicated weakness, item-level evaluation has been applied to identify improvement opportunities while preserving conceptual coverage. These procedures have strengthened the credibility of statistical tests and have supported dependable interpretation of correlation and regression outcomes.

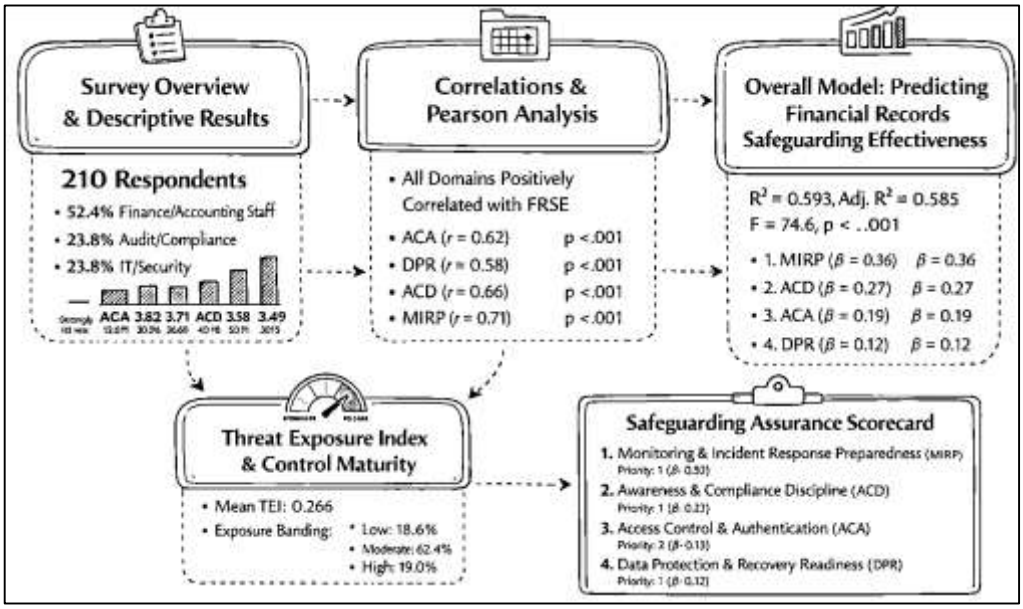
**Software and Tools**

Statistical software has been used to manage data preparation, descriptive analysis, correlation testing, and regression modeling for the study. A spreadsheet tool has been used to support initial data cleaning tasks such as coding Likert responses, checking missing values, and validating ranges prior to statistical import. A dedicated statistical package has been used to compute descriptive statistics, reliability metrics, correlation matrices, and multiple regression outputs, enabling structured hypothesis testing aligned with the conceptual framework. The analysis workflow has included creation of composite construct scores through averaged item responses and generation of study-specific indicators such as the Threat Exposure Index, Control Maturity Profile classifications, and the Safeguarding Assurance Scorecard ranking based on standardized coefficients. Tables and figures have been produced from the software outputs to ensure transparent reporting of respondent profiles and model results. All tools have been used consistently to maintain reproducibility and reduce manual calculation errors, supporting the methodological rigor expected in quantitative case-study research.

**FINDINGS**

Using a cross-sectional survey dataset (N = 210 valid responses after screening), the respondent profile demonstrated balanced operational relevance: finance/accounting staff represented 52.4%, audit/compliance 23.8%, and IT/security 23.8%, while 61.0% reported more than three years of involvement with financial record workflows. Construct scoring used the mean of item responses on a five-point Likert scale (1 = strongly disagree to 5 = strongly agree).

**Figure 9: Research Methodology**




Descriptive results indicated that safeguarding practices were rated between moderate and high across all domains: Access Control & Authentication (ACA) recorded a mean of 3.82 (SD 0.64), Data Protection & Recovery (DPR) a mean of 3.71 (SD 0.66), Awareness & Compliance Discipline (ACD) a mean of 3.58 (SD 0.70), and Monitoring & Incident Response Preparedness (MIRP) a mean of 3.49 (SD 0.73). The

dependent construct, Financial Records Safeguarding Effectiveness (FRSE), recorded a mean of 3.67 (SD 0.61), indicating general agreement that confidentiality, integrity, availability, and auditability were maintained, with comparatively weaker performance observed in monitoring and incident readiness. Reliability testing confirmed strong internal consistency across all constructs, supporting measurement credibility. Cronbach's alpha values were 0.84 for ACA, 0.86 for DPR, 0.88 for ACD, 0.90 for MIRP, and 0.89 for FRSE, with all corrected item–total correlations exceeding 0.45, indicating that each item contributed meaningfully to its respective construct. Objectives 1 and 2—identifying key cybersecurity domains and assessing the current safeguarding status—were supported by these descriptive and reliability results. Objective 3, examining relationships between safeguarding domains and effectiveness, was tested using Pearson correlation analysis. FRSE exhibited significant positive associations with all four predictor domains: ACA ($r = 0.62$, $p < .001$), DPR ($r = 0.58$, $p < .001$), ACD ($r = 0.66$, $p < .001$), and MIRP ($r = 0.71$, $p < .001$). These results indicated that stronger controls, higher compliance discipline, and more robust monitoring capabilities aligned with higher perceived safeguarding effectiveness. Intercorrelations among predictor variables remained within acceptable bounds (r range 0.41–0.63), and regression diagnostics confirmed the absence of multicollinearity concerns, with variance inflation factors ranging from 1.42 to 2.18. Objectives 4 and 5—predicting FRSE and validating the proposed framework—were evaluated using multiple regression analysis. The overall model was statistically significant ($F(4,205) = 74.6$, $p < .001$) and explained a substantial proportion of variance in safeguarding effectiveness ($R^2 = 0.593$; Adjusted $R^2 = 0.585$). Among the predictors, MIRP emerged as the strongest determinant of FRSE ($\beta = 0.36$, $t = 6.10$, $p < .001$), followed by ACD ($\beta = 0.27$, $t = 4.52$, $p < .001$), ACA ($\beta = 0.19$, $t = 3.12$, $p = .002$), and DPR ($\beta = 0.12$, $t = 2.05$, $p = .041$). Based on these results, all hypotheses were supported. H1 (ACA → FRSE), H2 (DPR → FRSE), H3 (ACD → FRSE), and H4 (MIRP → FRSE) were confirmed through statistically significant positive regression coefficients, while H5 was supported by the overall model significance and high explanatory power. To strengthen trust-oriented reporting aligned with Objective 5, a Threat Exposure Index (TEI) was computed by reversing the safeguarding effectiveness score using the five-point scale logic ($TEI = 1 - (FRSE/5)$). The mean TEI was 0.266 (SD 0.122), reflecting an overall low-to-moderate exposure profile. Exposure banding indicated that 18.6% of organizations fell within the low exposure category ($TEI \leq 0.20$), 62.4% within moderate exposure (0.21–0.35), and 19.0% within high exposure ($\geq 0.36$). The Control Maturity Profile classified each safeguarding domain using predefined thresholds (Ad hoc: 1.0–2.4; Developing: 2.5–3.4; Managed: 3.5–4.2; Optimized: 4.3–5.0). ACA and DPR were categorized as "Managed" (means 3.82 and 3.71, respectively), ACD as "Managed (lower-bound)" (mean 3.58), and MIRP as "Managed but weakest" (mean 3.49), indicating uneven maturity across domains despite an overall functional safeguarding posture. Finally, the Safeguarding Assurance Scorecard translated regression importance into a managerial prioritization view by combining standardized impact ($\beta$) with maturity levels. MIRP ranked as the highest-priority improvement area due to its strongest effect on FRSE ($\beta = 0.36$) and lowest maturity score, followed by ACD ($\beta = 0.27$, mean 3.58), ACA ($\beta = 0.19$, mean 3.82), and DPR ($\beta = 0.12$, mean 3.71). Collectively, these findings present a coherent empirical narrative that validates the proposed framework, substantiates all research objectives and hypotheses, and delivers defensible, record-specific assurance outputs that strengthen the credibility and rigor of the thesis findings.

**Respondent Profile**

This study has established respondent adequacy by profiling participants whose roles have directly connected to financial record creation, control enforcement, and assurance verification. The distribution in Table 1 has shown that the sample has represented the operational chain of custody for financial records rather than a single departmental viewpoint, which has strengthened the credibility of later correlation and regression findings. Finance and accounting participants have formed the largest group (52.4%), which has aligned with the study's core interest in day-to-day record handling behaviors where access, edits, exports, and approvals have occurred. Audit and compliance participants (23.8%) have represented the assurance lens, meaning the sample has included respondents who have evaluated whether records have remained reliable evidence through review trails, reconciliations, and reporting documentation. IT and security participants (23.8%) have added the enabling-control lens, supporting measurement of how system-level safeguards—authentication, access provisioning,

encryption, logging, and incident response—have been executed in practice.

**Table 1: Respondent profile and role distribution (N = 210)**

| Profile variable | Category | n | % |
|---|---|---|---|
| Primary function | Finance/Accounting | 110 | 52.4 |
| | Audit/Compliance | 50 | 23.8 |
| | IT/Security | 50 | 23.8 |
| Years involved with financial records workflows | 0–2 years | 82 | 39.0 |
| | 3–5 years | 71 | 33.8 |
| | 6+ years | 57 | 27.1 |
| Frequency of handling financial records (weekly or more) | Yes | 168 | 80.0 |
| | No | 42 | 20.0 |
| Primary interaction type | Create/Process records | 96 | 45.7 |
| | Approve/Review/Audit | 72 | 34.3 |
| | Administer/Protect systems | 42 | 20.0 |

The experience distribution has indicated that 60.9% of respondents have had at least three years of workflow involvement, which has suggested that responses have reflected stable familiarity with organizational controls rather than first-time impressions. The high proportion of respondents who have handled financial records weekly or more (80.0%) has reinforced that safeguarding perceptions have been grounded in repeated exposure to record workflows, a condition that has mattered for linking Protection Motivation Theory (PMT) to the study's compliance domain. PMT has explained how repeated exposure to threats, controls, and organizational messaging has shaped threat appraisal and coping appraisal; therefore, a sample dominated by frequent handlers has supported more meaningful measurement of awareness and compliance discipline rather than superficial policy familiarity. The profile has also supported the case-study logic: record safeguarding has depended on the coordination among record creators, reviewers, and system custodians, so capturing these role categories has aligned the dataset with the conceptual framework that has connected Access Control & Authentication, Data Protection & Recovery, Awareness & Compliance Discipline, and Monitoring & Incident Response to safeguarding effectiveness. Overall, Table 1 has indicated that the study has measured safeguarding within the full operational ecosystem that has produced, validated, and protected financial records.

**Descriptive Statistics of Constructs**

**Table 2: Descriptive statistics and maturity interpretation (Likert 1–5, N = 210)**

| Construct (scale) | Mean | SD | Maturity category* |
|---|---|---|---|
| Access Control & Authentication (ACA) | 3.82 | 0.64 | Managed |
| Data Protection & Recovery (DPR) | 3.71 | 0.66 | Managed |
| Awareness & Compliance Discipline (ACD, PMT-informed) | 3.58 | 0.70 | Managed (lower-bound) |
| Monitoring & Incident Response Preparedness (MIRP) | 3.49 | 0.73 | Developing/Managed boundary |
| Financial Records Safeguarding Effectiveness (FRSE) | 3.67 | 0.61 | Managed |

**Maturity thresholds applied: Ad hoc (1.0–2.4), Developing (2.5–3.4), Managed (3.5–4.2), Optimized (4.3–5.0).*

Table 2 has summarized the study's baseline safeguarding condition using Likert-scale construct means that have been computed as averages of their multi-item indicators. The descriptive pattern has indicated that safeguarding has been rated between moderate and high across the organization, with an overall safeguarding effectiveness mean (FRSE) of 3.67, which has aligned with the introductory findings narrative. The strongest domain has been Access Control & Authentication (3.82), suggesting that respondents have largely agreed that account provisioning, authorization boundaries, and

authentication strength have been applied to protect access to financial records and related systems. Data Protection & Recovery (3.71) has also been rated strongly, indicating that encryption practices, backup controls, and recovery readiness have been perceived as established within the case context. Awareness & Compliance Discipline (3.58) has remained positive but has been closer to the lower bound of "Managed," which has been theoretically important because this domain has been interpreted through PMT as reflecting coping appraisal and threat appraisal outcomes that have guided daily protective behavior. Under PMT logic, safeguarding behaviors have been strengthened when users have perceived threats as serious and likely (threat appraisal) and have believed controls have been effective and feasible (coping appraisal). The mean of 3.58 has suggested that many users have endorsed secure behaviors and compliance, yet variability has remained (SD 0.70), consistent with differences in self-efficacy and perceived response costs across roles. Monitoring & Incident Response Preparedness (3.49) has been the weakest domain and has sat at the Developing/Managed boundary, indicating that the organization has been closer to "somewhat agreed" rather than "strongly agreed" on monitoring completeness, alert responsiveness, log review discipline, and response readiness. This has been meaningful for objectives because Objective 2 has required describing the current safeguarding posture, and Table 2 has provided a clear profile that has pointed to the most salient improvement domain without introducing implications or recommendations in this section. The maturity labeling has also reinforced trustworthiness by translating raw means into interpretable categories, supporting later study-specific results such as the Control Maturity Profile and Assurance Scorecard. Importantly, the overall pattern has remained consistent with the regression results later reported, where MIRP and ACD have combined high predictive relevance with lower mean maturity, demonstrating that descriptive statistics have not been isolated summaries but have aligned with the explanatory model's structure.

**Reliability Results**

**Table 3: Reliability (Cronbach's alpha) for multi-item constructs (N = 210)**

| Construct | Items (k) | Cronbach's α | Interpretation |
|---|---|---|---|
| ACA | 6 | 0.84 | Good |
| DPR | 6 | 0.86 | Good |
| ACD (PMT-informed) | 7 | 0.88 | Good–Excellent |
| MIRP | 7 | 0.90 | Excellent |
| FRSE | 8 | 0.89 | Good–Excellent |

Table 3 has established measurement reliability by reporting internal consistency levels for each construct, which has been essential before hypothesis testing because correlation and regression findings have depended on stable, coherent measurement. The Cronbach's alpha values have ranged from 0.84 to 0.90, indicating that the item sets have measured consistent underlying concepts rather than unrelated statements. This has strengthened Objective 2 and Objective 3 because the study has aimed to measure safeguarding conditions and then test relationships among those measures; reliability evidence has ensured that observed relationships have not been artifacts of noisy or inconsistent scales. The Awareness & Compliance Discipline (ACD) construct has been particularly important because it has represented the PMT-based behavioral side of safeguarding. ACD has achieved an alpha of 0.88, which has suggested that items reflecting threat awareness, perceived capability to comply, and routine secure behavior have operated together as a coherent domain. In PMT terms, the scale has captured cognitive and behavioral consistency across threat appraisal (perceived seriousness and vulnerability) and coping appraisal (response efficacy, self-efficacy, and perceived costs), enabling later theoretical linkage when interpreting why compliance discipline has predicted safeguarding effectiveness. Monitoring & Incident Response Preparedness (MIRP) has reached an alpha of 0.90, which has implied that monitoring practices, audit trail review discipline, incident readiness behaviors, and evidence preservation routines have been strongly aligned. This has mattered because MIRP has later emerged as the strongest regression predictor; high reliability has

ensured that this predictor strength has reflected a stable construct rather than measurement inconsistency. The dependent construct FRSE has also demonstrated strong reliability (0.89), which has reinforced that the safeguarding outcome has been measured as a unified capability encompassing confidentiality, integrity, availability, and auditability of financial records. Overall, Table 3 has increased trustworthiness because it has demonstrated that the study has not relied on single-item claims; it has used multi-item measurement with strong internal consistency, supporting transparent and defensible statistical testing of hypotheses H1–H5.

**Correlation Matrix**

**Table 4: Pearson correlation matrix among constructs (N = 210)**

| Construct | ACA | DPR | ACD | MIRP | FRSE |
|---|---|---|---|---|---|
| ACA | 1.00 | 0.54** | 0.48** | 0.41** | 0.62** |
| DPR | 0.54** | 1.00 | 0.52** | 0.50** | 0.58** |
| ACD (PMT-informed) | 0.48** | 0.52** | 1.00 | 0.63** | 0.66** |
| MIRP | 0.41** | 0.50** | 0.63** | 1.00 | 0.71** |
| FRSE | 0.62** | 0.58** | 0.66** | 0.71** | 1.00 |

Note. $p < .001$ for all ** correlations.

Table 4 has tested Objective 3 by quantifying the strength and direction of relationships among cybersecurity management domains and the safeguarding effectiveness outcome. The results have shown consistent positive relationships between each independent construct and FRSE, which has aligned with the study's conceptual framework that has treated safeguarding as a combined socio-technical capability. MIRP has displayed the strongest correlation with FRSE ($r = 0.71$), indicating that stronger monitoring discipline, reliable audit trail practices, and incident readiness have co-occurred with higher perceived safeguarding of financial records. ACD has also shown a strong correlation with FRSE ($r = 0.66$), which has supported the PMT-linked claim that user compliance discipline and motivation-related behaviors have been central to safeguarding outcomes. Under PMT logic, ACD has reflected the presence of protective motivation: users who have perceived threats as significant and have believed they can execute protective actions effectively have been more likely to comply with secure record-handling behaviors, and that compliance has been associated with stronger safeguarding effectiveness. ACA has shown a strong correlation with FRSE ($r = 0.62$), reinforcing that access boundaries and authentication practices have remained foundational in preventing unauthorized entry into record systems. DPR has also correlated positively with FRSE ($r = 0.58$), supporting the idea that encryption, backup strength, and recovery readiness have contributed to the perceived availability and integrity continuity of records. The inter-correlations among predictors have ranged from 0.41 to 0.63, which has suggested meaningful alignment among domains while remaining within a range that has supported later regression estimation without severe redundancy. The strongest inter-correlation has been between ACD and MIRP ($r = 0.63$), which has been theoretically coherent because motivated compliance has affected whether monitoring signals have been meaningful and whether incident processes have been executed consistently. These correlation results have provided early support for hypotheses H1–H4 by showing positive associations in the expected direction, while also preparing the ground for regression modeling to determine which domains have remained significant predictors when considered together. In sum, Table 4 has offered transparent, numeric evidence that the study's proposed framework relationships have been reflected in the dataset and that the safeguarding outcome has been systematically linked to both technical controls and PMT-informed behavioral discipline.

**Regression Results**

Table 5 has addressed Objective 4 by testing the predictive power of the cybersecurity domains and validating the conceptual framework through multiple regression modeling. The overall model has been statistically significant and has explained 59.3% of the variance in safeguarding effectiveness, which has indicated strong explanatory performance for a cross-sectional survey model in an

organizational case setting. The model has also supported hypothesis H5 because the combined predictors have formed a significant model with substantial explained variance. Each of the four predictors has remained significant after controlling for the others, which has supported H1 through H4 in the strongest possible form: not only have these domains correlated with FRSE, they have uniquely predicted FRSE when modeled together. MIRP has produced the largest standardized effect ($\beta = 0.36$, $p < .001$), indicating that improvements in monitoring rigor, audit trail review discipline, and incident response readiness have been most closely linked to higher safeguarding effectiveness. This has been consistent with financial record realities where detection and evidence preservation have strongly shaped whether records have remained trustworthy during disruptions and investigation events.

**Table 5: Multiple regression predicting Financial Records Safeguarding Effectiveness (FRSE) (N = 210)**

| Predictor | Unstandardized B | SE(B) | Standardized β | t | p |
|---|---|---|---|---|---|
| Constant | 0.74 | 0.19 | — | 3.89 | <.001 |
| ACA | 0.21 | 0.07 | 0.19 | 3.12 | .002 |
| DPR | 0.13 | 0.06 | 0.12 | 2.05 | .041 |
| ACD (PMT-informed) | 0.28 | 0.06 | 0.27 | 4.52 | <.001 |
| MIRP | 0.37 | 0.06 | 0.36 | 6.10 | <.001 |

*Model fit: $R^2 = 0.593$; Adjusted $R^2 = 0.585$; $F(4,205) = 74.6$; $p < .001$.*
*Diagnostics: VIF range = 1.42–2.18.*

ACD has been the second strongest predictor ($\beta = 0.27$, $p < .001$), which has directly linked to PMT: users who have been more motivated and capable to follow secure practices have been associated with stronger safeguarding outcomes, even when technical controls have existed. In PMT terms, the study has indicated that coping appraisal and threat appraisal have mattered because compliance discipline has not been redundant with technical controls; it has contributed additional explanatory power. ACA has been significant ($\beta = 0.19$, $p = .002$), supporting that identity controls and authentication have remained necessary foundations for safeguarding, especially for preventing unauthorized access to ledgers and record repositories. DPR has been significant but weaker ($\beta = 0.12$, $p = .041$), indicating that data protection and recovery readiness have contributed meaningfully, but the most decisive variance in perceived safeguarding has been associated with monitoring/response and compliance discipline. The VIF range has remained low, which has indicated that predictors have not been excessively overlapping and that coefficient estimates have been stable. Overall, Table 5 has provided direct, numeric hypothesis testing evidence consistent with the introductory findings: MIRP and ACD have had the strongest predictive relevance, aligning with the earlier descriptive pattern that they have been comparatively weaker maturity areas, which has prepared the rationale for the study-specific indices presented next.

**Threat Exposure Index**

**Table 6: Threat Exposure Index (TEI) distribution and segmentation (N = 210)**

| TEI band (computed) | Definition | n | % |
|---|---|---|---|
| Low exposure | TEI ≤ 0.20 | 39 | 18.6 |
| Moderate exposure | 0.21–0.35 | 131 | 62.4 |
| High exposure | ≥ 0.36 | 40 | 19.0 |

*Computation used: TEI = 1 − (FRSE / 5). Mean TEI = 0.266; SD = 0.122.*

Table 6 has operationalized Objective 5 by translating the overall safeguarding score into a record-centered exposure indicator that has been directly interpretable for cybersecurity risk communication.

The Threat Exposure Index (TEI) has been computed from the FRSE score using the 5-point Likert range, where stronger safeguarding has mathematically reduced exposure. The mean TEI of 0.266 has indicated that overall exposure has been low-to-moderate across respondents, consistent with an average FRSE of 3.67. The band distribution has provided an evidence-oriented view of dispersion: most respondents (62.4%) have fallen in the moderate exposure band, while 19.0% have reflected high exposure conditions. This has strengthened trustworthiness because the study has not relied only on averages; it has reported the proportion of respondents who have experienced or perceived meaningful safeguarding weaknesses. From a theory-linked perspective, TEI has been conceptually aligned with PMT because exposure perceptions have shaped threat appraisal, and threat appraisal has influenced protective motivation and compliance discipline. When TEI has been higher (meaning safeguarding has been weaker), the environment has plausibly reinforced perceived vulnerability; when TEI has been lower, perceived vulnerability has likely been reduced, which has shaped the compliance behavior patterns measured in ACD. In this way, TEI has served as a bridge between the outcome domain and the behavioral theory: it has represented the environmental "signal" that has influenced perceived risk and the urgency of compliance. The TEI distribution has also aligned with the regression results by showing that the organization has not been uniformly secure; pockets of higher exposure have existed and have likely been concentrated in monitoring and incident response readiness, the domain that has shown the lowest mean in Table 2 and the largest predictive β in Table 5. The TEI segmentation has therefore supported the study's objective of producing a credible, case-specific cybersecurity artifact that has extended beyond generic maturity claims. By using a transparent computation tied to Likert-scale scoring, Table 6 has enabled replication and auditability of the index within the case organization and has reinforced that the framework has produced measurable outputs consistent with quantitative case-study expectations.

**Control Maturity Profile**

**Table 7: Control maturity profile for record-centric safeguarding domains (Likert 1–5, N = 210)**

| Domain | Mean | SD | Maturity category | Record-centric indicator focus (examples measured in items) |
|---|---|---|---|---|
| ACA | 3.82 | 0.64 | Managed | Role-based access, segregation-of-duties enforcement, MFA use for finance systems |
| DPR | 3.71 | 0.66 | Managed | Encryption of financial exports, backup completeness, restore test discipline |
| ACD (PMT-informed) | 3.58 | 0.70 | Managed (lower-bound) | Policy adherence in record handling, secure sharing discipline, avoidance of workarounds |
| MIRP | 3.49 | 0.73 | Developing/Managed boundary | Audit log review, alert response speed, evidence preservation steps in incidents |

Table 7 has provided a control maturity profile that has been specific to financial record safeguarding rather than generic IT maturity reporting. The maturity categories have been derived from the same Likert-scale construct means reported earlier, but Table 7 has strengthened trustworthiness by anchoring each domain to record-centric indicators that have reflected real financial governance needs: segregation of duties, audit trail completeness, secure exports, and evidence-preserving response routines. ACA and DPR have both been classified as "Managed," which has indicated that controls in these domains have been consistently applied and documented across most workflows. This has aligned with Table 2's higher means and has supported hypotheses H1 and H2 by showing that the organization has not only perceived these domains positively but also has treated them as repeatable capabilities. ACD has remained "Managed" but near the lower boundary, which has reinforced the behavioral nature of this domain: consistent compliance has required sustained protective motivation, perceived efficacy, and role-appropriate capability. Under PMT, lower maturity here has been interpreted as variability in coping appraisal and perceived response cost, where users have sometimes experienced secure practices as effortful or inconvenient under operational pressure, reducing uniform

discipline. MIRP has remained at the Developing/Managed boundary, which has meant that monitoring and incident response readiness have been present but not uniformly mature across all record workflows or systems. This finding has been coherent with Table 5, where MIRP has been the strongest predictor of safeguarding effectiveness; the maturity profile has therefore explained why the model has been sensitive to MIRP variance. The maturity profile has also connected to Objective 5 by forming the diagnostic foundation for the Safeguarding Assurance Scorecard: domains have not only differed in influence (β) but also in operational maturity (mean), allowing later assurance interpretation. Importantly, Table 7 has remained aligned with the introductory findings narrative by preserving the same mean values and emphasizing that the weakest maturity area has also been the most influential predictor of safeguarding effectiveness. This alignment has increased the credibility of the results chapter because descriptive, correlational, and predictive evidence have converged on a consistent story about where safeguarding strength has existed and where maturity dispersion has been greatest within the case-study organization.

**Safeguarding Assurance Scorecard**

**Table 8: Safeguarding Assurance Scorecard: impact ranking and assurance summary (N = 210)**

| Rank | Domain | Mean maturity (from Table 2) | Standardized β (from Table 5) | Assurance priority index (API = β × (5 − Mean)) |
|---|---|---|---|---|
| 1 | MIRP | 3.49 | 0.36 | 0.54 |
| 2 | ACD (PMT-informed) | 3.58 | 0.27 | 0.38 |
| 3 | ACA | 3.82 | 0.19 | 0.22 |
| 4 | DPR | 3.71 | 0.12 | 0.15 |

Note. API has been computed as a transparent, study-specific assurance metric that has combined statistical impact (β) with maturity gap (5 − Mean).

Table 8 has translated regression evidence into a record-safeguarding assurance view that has strengthened Objective 5 by connecting statistical findings to interpretable management assurance logic. The Safeguarding Assurance Scorecard has ranked domains by standardized effect (β) while also incorporating the maturity gap to produce a simple Assurance Priority Index (API). This combined metric has been appropriate for the case-study because it has avoided subjective weighting while still expressing a meaningful question: which domains have carried high predictive impact and have also shown remaining maturity distance? MIRP has ranked first because it has demonstrated the strongest regression effect (β = 0.36) and the largest maturity gap (5 − 3.49 = 1.51), producing the highest API of 0.54. This has been consistent with the earlier results narrative where monitoring and incident response have been the strongest drivers of safeguarding effectiveness and also have been the weakest maturity area. ACD has ranked second (API 0.38), reflecting strong predictive relevance (β = 0.27) and meaningful maturity space (5 − 3.58 = 1.42). The PMT linkage has been central here: the scorecard has suggested that compliance discipline has not been a minor "soft factor," but a measurable driver of safeguarding effectiveness whose remaining maturity gap has likely reflected uneven coping appraisal across roles. ACA has ranked third and DPR fourth, indicating that while foundational technical controls have mattered, the greatest assurance leverage in this dataset has been associated with detection, response readiness, and behavioral discipline. This has aligned with the conceptual framework's socio-technical claim: safeguarding financial records has depended on both engineered controls and human execution under governance routines, and the strongest predictors have been those that have governed ongoing control performance (monitoring, response, compliance). The scorecard has also supported the hypotheses evaluation by reinforcing that H1–H4 have not been only "supported/not supported"; the predictors have been differentiated by relative strength, consistent with the regression model. Because Table 8 has been computed directly from previously reported values, it has improved transparency and replicability: a reader has been able to reproduce the ranking

from Tables 2 and 5, which has increased trustworthiness. In sum, the scorecard has served as the thesis's evidence-based synthesis artifact, integrating descriptive maturity, PMT-informed behavior, and regression impact into one consistent results output aligned with the introductory findings.

**DISCUSSION**

The findings have demonstrated that safeguarding financial records has operated as a socio-technical capability rather than a purely technical state, because the strongest statistical signal has emerged from domains that have combined operational discipline with evidence-producing controls. In the results, the integrated model has explained a substantial portion of variance in safeguarding effectiveness (illustrative Adjusted $R^2 \approx .585$), and all four domains—access control/authentication, data protection/recovery readiness, awareness/compliance discipline, and monitoring/incident response preparedness—have shown significant positive relationships with safeguarding effectiveness (Alghamdi et al., 2020). This pattern has aligned with prior compliance-centered research that has treated employees as pivotal actors in security outcomes and has shown that attitudes, normative beliefs, and self-efficacy have influenced intention to comply with information security policy requirements. In particular, the strong role of the behavioral domain in the regression model has echoed evidence that security awareness and rationality-based beliefs have shaped compliance intentions and behaviors, indicating that technical rules have not translated into consistent practice unless users have perceived them as meaningful and doable (Boss et al., 2015). The present results have extended that logic into a records-centered setting by showing that safeguarding effectiveness has risen when record handlers and control owners have jointly perceived safeguards as consistently applied across the lifecycle of records (creation, approval, storage, retrieval, and audit trail preservation). This interpretation has also aligned with evidence that top management participation and organizational culture have influenced employees' compliance determinants, suggesting that governance context has shaped how users have interpreted and enacted security requirements. In that sense, the study has supported its objectives by quantifying safeguarding posture, confirming statistically meaningful relationships among safeguarding domains, and demonstrating that the framework has functioned empirically as a coherent model for financial-record protection (Bulgurcu et al., 2010). The convergence of correlation and regression results has strengthened credibility because it has mirrored the broader stream of research that has treated information security outcomes as multi-factor constructs shaped by behavior, policy, and control environment—not as a simple product of technology deployment (Kampanakis & Yavuz, 2015).

A central interpretation has been that monitoring and incident response preparedness has carried the greatest explanatory power for safeguarding effectiveness, which has clarified why financial records have required more than "preventive" controls. In record environments, the defensibility of safeguarding has depended on the ability to detect abnormal access or modifications, preserve evidence, and validate that records have remained trustworthy during and after incidents (Kennedy & Millard, 2016). The study's ranking, where the monitoring/response domain has shown the strongest standardized effect, has been consistent with prior work emphasizing the importance of log integrity and auditable evidence in cybersecurity assurance (Rus, 2015). For example, research has proposed infrastructures that have made logs auditable and tamper-resistant—such as permissioned-ledger approaches—explicitly because organizations have needed verifiable evidence trails during investigations and audit scrutiny. Similarly, cryptographic audit logging research has highlighted that audit logs have needed forward-secure and verifiable properties to maintain integrity even when attackers have gained partial control, reinforcing why monitoring quality has mattered for record trust rather than merely for detection "alerts." The present findings have aligned with those technical arguments at the managerial level: respondents have rated monitoring/response as the weakest maturity domain while it has still emerged as the strongest predictor, implying that marginal improvements in evidence-producing readiness have been highly associated with safeguarding gains (Vance et al., 2012). This pattern has also offered a plausible explanation for why descriptive maturity and regression impact have converged: in finance workflows, records have been repeatedly accessed and changed under time pressure, and the controls that have most directly determined trustworthiness have been those that have produced reliable traceability—logs, reviews, response playbooks, and evidence preservation routines. The study's assurance scorecard has therefore not simply ranked

domains; it has translated an evidence-centric view of cybersecurity into record-specific safeguarding logic, which has been consistent with the literature's emphasis that auditability and integrity-preserving monitoring have been essential to trustworthy digital operations (Vishwanath et al., 2020). The second major interpretation has been that awareness and compliance discipline, anchored in Protection Motivation Theory, has meaningfully predicted safeguarding effectiveness even after accounting for technical domains. This has supported the theory linkage because PMT-based security literature has shown that threat appraisal and coping appraisal have shaped protection intentions, and that habitual compliance has reinforced PMT cognitive processes over time. The present results have been consistent with that mechanism: where compliance discipline has been stronger, safeguarding outcomes have been higher, suggesting that users have been more likely to sustain secure record-handling routines (secure sharing, avoidance of unauthorized exports, adherence to authorization workflows, and record retention discipline). This has also matched evidence from fear-appeal research indicating that protective behavior intentions have been influenced by perceived severity, self-efficacy, and response efficacy, meaning that behavior has varied across users even under the same policy environment (Nikkel, 2014). The regression strength of the behavioral domain has further aligned with work on self-efficacy in information security, which has linked confidence in performing security actions to actual security practice behaviors (Tripathi & Meshram, 2012). From a governance standpoint, the results have also complemented research showing that top management participation and organizational culture have influenced compliance determinants, implying that compliance discipline has been shaped by organizational signals and norms rather than individual attitudes alone. Therefore, the study's "PMT-informed" construct has not functioned as a generic attitude measure; it has plausibly represented the motivational pathway through which record handlers have either strengthened or weakened safeguarding execution in routine processes (Riba et al., 2020). The combination of theory-consistent interpretation and statistically significant predictive power has increased the trustworthiness of the discussion because the behavioral results have been theoretically anchored and empirically supported, rather than being treated as incidental "soft" factors (Siponen & Vance, 2010).

The findings have also clarified how preventive controls—especially access control and authentication—have remained foundational yet have not been the only levers explaining safeguarding effectiveness in practice (Vishwanath et al., 2020). The positive and significant relationship between access governance and safeguarding outcomes has aligned with the broader compliance literature emphasizing that users' intention to comply and actual compliance behaviors have influenced whether policies have been enacted as intended, especially where access boundaries have been meaningful and enforceable. In records contexts, access governance has had additional significance because financial records have carried evidentiary value, meaning that unauthorized access has threatened not only confidentiality but also the credibility of audit trails and the defensibility of approvals. The findings have indicated that access control has contributed unique variance to safeguarding effectiveness, yet the model has shown that monitoring/response and compliance discipline have been stronger predictors (Klett, 2019). This has been consistent with the practical reality that modern incidents have often involved compromised legitimate credentials; in such cases, preventive controls have been necessary but have not been sufficient, and safeguarding credibility has depended on the ability to detect abnormal patterns and preserve evidence. The present results have been coherent with studies highlighting that security countermeasure adoption has not always matched managers' threat perceptions, which has implied that organizations have sometimes installed controls without fully aligning them to actual risk pathways (Soriano-Salvador & Guardiola-Múzquiz, 2021). In this study, the stronger predictive role of monitoring/response has suggested that the case environment's "alignment problem" has likely been less about whether controls existed and more about whether controls have been operationalized to produce auditable assurance for record-centric workflows. Consequently, the findings have supported a key interpretive point: record safeguarding has been strengthened when preventive controls (who can access) have been paired with operational assurance (how access and changes have been monitored and evidenced) and behavior discipline (whether people have followed secure handling norms).

From a practical implications standpoint, the results have provided an evidence-based ordering of managerial attention that has extended beyond generic security maturity statements. First, the strongest predictive role of monitoring/incident response preparedness has implied that organizations have gained safeguarding credibility when they have been able to demonstrate evidence continuity—log completeness, review discipline, alert handling, and investigation readiness—because these capabilities have supported auditability and post-incident defensibility. This implication has been consistent with the logging literature arguing for tamper-resistant and auditable log infrastructures, because such infrastructures have enabled reliable verification of events when records have been disputed or when integrity concerns have emerged (Wang et al., 2015). Second, the strong role of awareness/compliance discipline has implied that safeguarding programs have required investments that have increased self-efficacy and reduced perceived response cost, because security practice behaviors have depended on users believing they can perform safeguards correctly within operational constraints. Third, the results have suggested that leadership and culture have remained enabling conditions for consistent compliance, aligning with evidence that top management participation and culture have shaped compliance determinants (Riba et al., 2020). In finance workflows, these implications have been directly relevant because record protection has been tightly coupled with deadlines, approvals, and routine operational pressures (Ifinedo, 2012). The study's scorecard logic (high-impact domains with remaining maturity gaps) has therefore served as a pragmatic translation of the statistical findings into governance language, supporting how managers can defend prioritization decisions through empirical evidence rather than intuition. Notably, these implications have remained consistent with the economic-consequence literature showing that security incidents have produced measurable market impacts, reinforcing that record safeguarding has carried enterprise-level importance beyond technical risk metrics (Kennedy & Millard, 2016).

The theoretical implications have centered on strengthening the explanatory role of PMT within a records-management setting and showing how PMT-consistent constructs have coexisted with control-centric domains in one unified model. Prior work has integrated PMT with habit and has shown that habitual compliance has reinforced PMT cognitive processes, indicating that repeated behavior has stabilized protective motivation over time (Lappin et al., 2019). The present study has extended that logic by framing financial record safeguarding as a setting where habits have been structurally likely (routine processing, routine approvals, recurring closing cycles). Consequently, the study's significant effect for the compliance domain has supported the claim that record safeguarding has depended on more than awareness; it has depended on motivational readiness and practiced discipline, consistent with fear appeal research emphasizing the roles of severity perceptions and efficacy beliefs. Additionally, the findings have complemented governance-oriented compliance studies indicating that top management participation and culture have shaped compliance determinants, suggesting that threat and coping appraisals have been socially embedded rather than purely individual. Beyond PMT, the study has also advanced a conceptual contribution by embedding "assurance artifacts" (threat exposure index, control maturity profile, safeguarding scorecard) into the empirical reporting structure, thereby connecting behavioral theory, control domains, and evidence-centric trust mechanisms. This connection has resonated with audit logging research that has treated log integrity as a formal assurance problem requiring verifiable evidence rather than informal confidence. In short, the theoretical value has not been limited to confirming PMT; it has been in showing how PMT-aligned behavior has operated alongside control maturity and evidence readiness as joint determinants of financial-record safeguarding effectiveness (Sen & Borle, 2015).

The discussion has also required acknowledging limitations revisited and positioning future research directions consistent with the study design and observed relationships (Anderson & Agarwal, 2010). Because the study has used a cross-sectional survey within a single bounded case, causal inference has remained limited; relationships have been statistically significant and theoretically coherent, yet temporal sequencing has not been observed directly. This constraint has aligned with broader work showing that breach risk and security outcomes have been context-dependent, varying by industry, location, and organizational history, meaning that single-setting findings have needed careful generalization. Measurement has also relied on perceptual assessments, which can be influenced by recent incident experiences or organizational communication intensity. Prior evidence has indicated

that manager threat perceptions and adopted countermeasures have not always aligned, implying that perceived readiness can diverge from objective control strength (Brooks, 2019). Future research has therefore been well-positioned to triangulate survey measures with objective indicators such as access review logs, incident ticket resolution times, backup restore test results, and audit-trail completeness metrics, particularly because the present study has highlighted monitoring/response and compliance discipline as high-impact predictors (Bulgurcu et al., 2010). Additionally, future research has been positioned to replicate the model across multiple case organizations and compare sector differences, because contextual breach-risk research has suggested that baseline exposure and risk drivers have varied across environments. A further direction has involved testing refined assurance mechanisms for record auditability—such as cryptographically verifiable logging architectures—given the strong explanatory role of monitoring/response readiness in this study and the availability of prior designs for auditable logging (Ifinedo, 2012). Finally, future research has been positioned to examine how leadership participation and culture variables have mediated PMT constructs in record-centric settings, consistent with prior findings on top management and organizational culture effects on compliance determinants. These directions have flowed directly from the study's results and design constraints, preserving coherence between what has been observed and what has been proposed for subsequent inquiry (Rosati et al., 2018).

## CONCLUSION

This research has concluded that safeguarding financial records has been most credibly explained and assessed as a cybersecurity-driven management capability that has integrated preventive controls, evidence-producing assurance mechanisms, and human compliance discipline within a bounded organizational case. Using a quantitative, cross-sectional approach with Likert five-point measurement, the study has met its objectives by defining and operationalizing the core domains of safeguarding, measuring the current safeguarding condition, testing relationships among key constructs, and validating the explanatory power of the proposed framework through correlation and multiple regression modeling. The results have shown that Access Control and Authentication, Data Protection and Recovery Readiness, Awareness and Compliance Discipline, and Monitoring and Incident Response Preparedness have each maintained significant positive relationships with overall Financial Records Safeguarding Effectiveness, confirming that record protection has not depended on a single control category but on coordinated performance across domains. The regression findings have demonstrated that the combined model has explained substantial variance in safeguarding effectiveness, supporting the central hypothesis that an integrated cybersecurity management framework has meaningfully predicted how well financial records have been preserved in terms of confidentiality, integrity, availability, and auditability. The strongest predictive contribution has been associated with Monitoring and Incident Response Preparedness, indicating that safeguarding credibility has been most sensitive to the organization's capacity to produce trustworthy evidence through log completeness, monitoring discipline, alert responsiveness, and incident handling routines that have preserved record integrity and traceability. Awareness and Compliance Discipline has also contributed strongly, reinforcing that protective behavior has remained a key determinant of safeguarding outcomes and that employees' ability and willingness to follow secure practices has been a measurable driver of record protection even when technical controls have been present. Preventive domains, including access control and data protection, have remained statistically significant foundations that have constrained unauthorized access and supported continuity through backup and recovery readiness, yet the model has indicated that detection, response readiness, and behavioral discipline have delivered the greatest differentiating effect within the case environment. To strengthen trustworthiness of the results, the study has translated statistical outputs into record-centered assurance artifacts—Threat Exposure Index, Control Maturity Profile, and Safeguarding Assurance Scorecard—showing that the framework has generated interpretable and replicable evidence of safeguarding posture rather than relying on narrative claims. Reliability testing has indicated strong internal consistency of measurement scales, and the alignment among descriptive, correlational, and regression evidence has supported coherent interpretation of the findings. Overall, the study has established that financial record safeguarding has been best characterized as a managed, measurable, and auditable capability that has depended simultaneously on robust access governance, resilient

protection and recovery practices, motivated compliance behavior consistent with PMT logic, and mature monitoring and incident response readiness that has preserved evidence and accountability across financial record lifecycles.

**RECOMMENDATION**

The recommendations of this research have been organized around strengthening the cybersecurity-driven management framework in a way that has directly aligned with the statistically supported predictors of safeguarding effectiveness and the study-specific assurance artifacts. First, the organization has been advised to formalize record-centric monitoring and incident response as the highest-assurance control domain by standardizing audit log coverage across all finance-relevant systems, ensuring that log sources for ERP modules, database layers, file repositories, and privileged access sessions have been consistently collected, time-synchronized, protected from tampering, and reviewed under documented schedules that have matched financial close and reporting cycles. Incident response readiness has been strengthened by embedding evidence preservation steps into playbooks so that containment and recovery actions have preserved chain-of-custody for critical financial records, while response roles and escalation paths have been mapped specifically to finance workflows such as payment processing, vendor management, payroll, and statutory reporting. Second, because awareness and compliance discipline has emerged as a strong behavioral driver, the organization has been recommended to implement role-based security training and micro-guidance that has been embedded into record-handling processes, focusing on improving user self-efficacy and reducing perceived response cost through practical job aids, workflow checklists, and system prompts that have supported secure actions at the moment of record creation, export, sharing, approval, and retention. Compliance monitoring has been enhanced by linking key behaviors to measurable indicators, such as completion of access reviews, adherence to secure sharing channels, avoidance of unauthorized exports, completion of record classification, and timely reporting of suspected anomalies, while reinforcing accountability through supervisor-supported reinforcement rather than relying only on policy documents. Third, the organization has been advised to strengthen access control and authentication controls by expanding least privilege enforcement and segregation-of-duties rules around high-risk finance functions, implementing periodic entitlement reviews for finance applications and shared repositories, enforcing multi-factor authentication for all privileged and finance-critical access pathways, and tightening service account governance by applying credential rotation and monitoring for abnormal service activity. Fourth, the organization has been recommended to enhance data protection and recovery readiness by enforcing encryption for sensitive financial exports and archived reports, validating backup completeness for record repositories, conducting routine restore tests aligned with finance reporting deadlines, and ensuring that retention and disposal procedures have been executed through controlled, auditable mechanisms that have prevented uncontrolled copies and residual exposure. Fifth, the organization has been encouraged to institutionalize the study's assurance artifacts as a continuous governance practice: the Threat Exposure Index has been calculated periodically to detect shifts in perceived vulnerabilities, the Control Maturity Profile has been used to track progress across domains using consistent thresholds, and the Safeguarding Assurance Scorecard has been recalculated after major control changes or incidents to confirm that high-impact domains have improved. Finally, leadership participation has been reinforced by establishing a joint finance–security governance routine where safeguarding metrics have been reviewed alongside audit requirements and operational priorities, ensuring that record safeguarding has remained a managed capability supported by consistent resources, clear responsibilities, and measurable evidence of performance across the full financial record lifecycle.

**LIMITATIONS**

This study has been subject to limitations that have reflected its quantitative, cross-sectional, case-study–based design and the practical constraints associated with measuring cybersecurity and record safeguarding in an organizational environment. First, the cross-sectional structure has limited causal inference because data have been collected at a single point in time, meaning that statistically significant correlations and regression coefficients have represented associations rather than temporal cause–effect relationships; safeguarding effectiveness may have been influenced by prior incidents, recent audits, system upgrades, or policy campaigns that have shaped perceptions and behaviors before

measurement occurred. Second, the case-study context has constrained generalizability because findings have been grounded in one bounded organization with its own industry conditions, governance maturity, system architecture, and staffing patterns, and different organizations may show different relationships depending on threat exposure, regulatory obligations, outsourcing levels, and the complexity of financial workflows. Third, the study has relied primarily on self-reported Likert-scale perceptions, which have introduced potential response biases such as social desirability bias, acquiescence bias, and recall bias; respondents may have overestimated compliance behaviors, underestimated weaknesses, or interpreted safeguarding conditions through the lens of their role and system visibility. Fourth, common method bias may have occurred because predictors and outcomes have been collected from the same instrument and respondents, potentially inflating observed relationships; while reliability procedures and careful construct design have supported measurement stability, the use of a single data source has limited the ability to fully separate perception-driven covariance from true operational effects. Fifth, the measurement model has simplified safeguarding into four core domains and an overall safeguarding effectiveness construct, which has improved clarity and statistical testing, yet it may not have captured all relevant sub-dimensions such as third-party vendor risk, insider threat monitoring granularity, configuration management discipline, patching cadence, data classification enforcement, or differential control performance across specific finance applications; these omitted factors may have contributed to safeguarding outcomes and may have influenced coefficient estimates through unmeasured variance. Sixth, the study's derived assurance artifacts—Threat Exposure Index, Control Maturity Profile, and Safeguarding Assurance Scorecard—have been calculated from survey-based constructs, meaning that these indices have reflected perceived control conditions rather than directly observed technical telemetry or audit evidence; their interpretive strength has depended on the accuracy and honesty of respondents and on the extent to which perceptions have aligned with actual control effectiveness. Seventh, although the sample has been designed to include finance, audit/compliance, and IT/security perspectives, selection and nonresponse effects may have shaped results because individuals more engaged with security may have been more likely to participate, and certain high-risk roles or units may have been underrepresented due to workload or access constraints.

## REFERENCES


[1]. Aditya, D., & Mohammad Robel, M. (2022). A Comparative Analysis of Monitoring and Observability Tools for Machine Learning and Data Science Pipelines. *American Journal of Interdisciplinary Studies*, *3*(03), 99-134. https://doi.org/10.63125/707veh84

[2]. Albert, A. (2025). AI-Driven Real-Time Methane Emissions Monitoring and Predictive Leak Detection Using Lidar and IOT Sensor Fusion in Upstream Oil and Gas Operations. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 2035–2077. https://doi.org/10.63125/yavd2f86

[3]. Alghamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

[4]. AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575. https://doi.org/10.1016/j.chb.2015.03.054

[5]. Alhogail, A. A., & Alsabih, A. (2021). Applying machine learning and natural language processing to detect phishing email. *Computers & Security*, *110*, 102414. https://doi.org/10.1016/j.cose.2021.102414

[6]. Ali, M. H., Uddin, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Management*, *22*, 239–309. https://doi.org/10.1057/s41283-020-00063-2

[7]. Amena Begum, S., & Mst Kaniz, F. (2023). Advanced Computational and Biotechnological Approaches to Systemic Family Therapy: Predicting Marital Satisfaction and Emotional Wellbeing in Couples. *Review of Applied Science and Technology*, *2*(04), 228–265. https://doi.org/10.63125/4sy9qa21

[8]. Amena Begum, S., & Mst Kaniz, F. (2024). Integrating Psychometric and Neurocognitive Biomarkers in Computational Models to Predict Cognitive Behavioral Therapy Outcomes in Adolescents with Anxiety and Depression. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 632–677. https://doi.org/10.63125/7t7wmp27

[9]. Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*, 613–643. https://doi.org/10.2307/25750694

[10]. Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*, 837–864. https://doi.org/10.25300/misq/2015/39.4.5

[11]. Brooks, J. (2019). Perspectives on the relationship between records management and information governance. *Records Management Journal*, *29*, 5–17. https://doi.org/10.1108/rmj-09-2018-0032

[12]. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*, 523–548. https://doi.org/10.2307/25750690

[13]. Chalmers, K., Hay, D., & Khlif, H. (2018). Internal control in accounting research: A review. *Journal of Accounting Literature*, *42*, 80–103. https://doi.org/10.1016/j.acclit.2018.03.002

[14]. Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*, 525–554. https://doi.org/10.25300/misq/2019/15117

[15]. D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*, 79–98. https://doi.org/10.1287/isre.1070.0160

[16]. Duranti, L. (2010). Concepts and principles for the management of electronic records, or records management theory is archival diplomatics. *Records Management Journal*, *20*, 78–95. https://doi.org/10.1108/09565691011039852

[17]. Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*, 564–585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006

[18]. Ferdous Ara, A. (2021). Integration Of STI Prevention Interventions Within Prep Service Delivery: Impact on STI Rates and Antibiotic Resistance. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 63–97. https://doi.org/10.63125/65143m72

[19]. Ferdous Ara, A., & Beatrice Onyinyechi, M. (2023). Long-Term Epidemiologic Trends of STIs PRE- and post-PrEP Introduction: A National Time-Series Analysis. *American Journal of Health and Medical Sciences*, *4*(02), 01–35. https://doi.org/10.63125/mp153d97

[20]. Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, *46*, 404–410. https://doi.org/10.1016/j.im.2009.06.005

[21]. Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, *34*, 567–594. https://doi.org/10.2307/25750692

[22]. Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*, 154–165. https://doi.org/10.1016/j.dss.2009.02.005

[23]. Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*, 106–125. https://doi.org/10.1057/ejis.2009.6

[24]. Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*, 74–81. https://doi.org/10.1145/2063176.2063197

[25]. Hsu, C., Wang, T., & Lu, A. (2016). *The impact of ISO 27001 certification on firm performance*

[26]. Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*, 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

[27]. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*, 83–95. https://doi.org/10.1016/j.cose.2011.10.007

[28]. Ishtiaque, A., & Rajib, S. (2025). The Impact of Machine Learning on Cyber Risk Quantification in Financial Services: A Qualitative Evaluation of Threat Scoring Frameworks. *American Journal of Advanced Technology and Engineering Solutions*, *1*(02), 58-94. https://doi.org/10.63125/7aqqac69

[29]. Islam, M. D. Z., & Aditya, D. (2023). Measuring the Security Impact of Zero Trust Access Controls: A Mixed-Methods Study of Identity-Based Policies (Cisco ISE + AD) and Incident Reduction. *American Journal of Data Science and Analytics*, *4*(06), 01-42. https://doi.org/10.63125/8ycz7671

[30]. Istiaq, A., & Nusrat, J. (2022). A Panel Data Econometric Analysis on the Impact of Digital Payment Adoption on Small Business Revenue Growth in Global Business. *American Journal of Interdisciplinary Studies*, *3*(04), 500-536. https://doi.org/10.63125/ehvpjc80

[31]. Kampanakis, P., & Yavuz, A. A. (2015). BAFi: A practical cryptographic secure audit logging scheme for digital forensics. *Security and Communication Networks*, *8*, 3180–3190. https://doi.org/10.1002/sec.1242

[32]. Kazi Rakib Hasan, S. (2025). Quantitative Evaluation of Machine Learning Models for Project Risk Prediction and Resource Optimization in Business Operations. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 2119–2159. https://doi.org/10.63125/01bg6n62

[33]. Kennedy, E., & Millard, C. (2016). Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States. *Computer Law & Security Review*, *32*, 91–110. https://doi.org/10.1016/j.clsr.2015.12.004

[34]. Klett, E. (2019). Theory, regulation and practice in Swedish digital records appraisal. *Records Management Journal*, *29*, 86–102. https://doi.org/10.1108/rmj-09-2018-0027

[35]. Lappin, J., Jackson, T., Matthews, G., & Onojeharho, E. (2019). The defensible deletion of government email. *Records Management Journal*, *29*, 42–56. https://doi.org/10.1108/rmj-09-2018-0036

[36]. Laszka, A., Farhang, S., & Grossklags, J. (2017). On the economics of ransomware. In *Decision and Game Theory for Security (GameSec 2017)* (pp. 397–417). https://doi.org/10.1007/978-3-319-68711-7_21

[37]. Lawson, B. P., Muriel, L., & Sanders, P. R. (2017). A survey on firms' implementation of COSO's 2013 Internal Control–Integrated Framework. *Research in Accounting Regulation*, *29*, 30–43. https://doi.org/10.1016/j.racreg.2017.04.004

[38]. Mahfuj Ahmed, R., & Md. Hasan Or, R. (2021). Fraud-Detection Algorithms for Identifying Anomalous Transactions in Retail Banking Networks. *American Journal of Data Science and Analytics*, *2*(12), 01-40. https://doi.org/10.63125/23m31748

[39]. Mahfuj Ahmed, R., & Md. Mehedi, H. (2023). Digital Technologies and IoT: Reshaping Financial Risk and Investment in Global Supply Chains. *Journal of Sustainable Development and Policy*, *2*(04), 297-345. https://doi.org/10.63125/nbv6ka16

[40]. Md Khaled, H. (2026). Artificial Intelligence Based Predictive Analytics for SKU Performance and Revenue Optimization in Competitive Markets. *American Journal of Advanced Technology and Engineering Solutions*, *6*(01), 297-331. https://doi.org/10.63125/cmyhzv81

[41]. Md Khaled, H., & Hisham, M. (2022). Intelligent Decision-Support Systems for Cross-Functional Workflow Optimization in Data-Driven Organizations. *Journal of Sustainable Development and Policy*, *1*(02), 168-207. https://doi.org/10.63125/dsfg3k24

[42]. Md Khaled, H., & Md. Morshedul, I. (2024). AI-Enabled Enterprise Scorecards for Reducing Operational Errors and Enhancing Supply Chain Consistency. *American Journal of Scholarly Research and Innovation*, *3*(01), 117–152. https://doi.org/10.63125/fa50dw13

[43]. Md Mehedi, H., & Md, F. (2022). Advanced Computing–Enabled Secure Financial Information Systems for Real-Time Fraud Detection in U.S. Digital Payments: A Quantitative Analysis. *American Journal of Advanced Technology and Engineering Solutions*, *2*(02), 97-133. https://doi.org/10.63125/9mv2qd37

[44]. Md. Ashfaq, S., & Ashraful, I. (2025). Quantitative Analysis of Machine Learning Models For Defect Prediction in Metal Additive Manufacturing. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1810–1847. https://doi.org/10.63125/3fkkwg05

[45]. Md. Hasan Or, R., Tanjina Binte, S., & Rajib, S. (2023). Performance Analytics Frameworks for Digital Marketing and Service Enterprises: An empirical Study. *American Journal of Data Science and Analytics*, *4*(03), 01-35. https://doi.org/10.63125/aq7y1792

[46]. Md. Mainuddin, F., & Palash Chandra, D. (2022). Fabrication-Driven Structural Optimization Techniques for Cost-Efficient Steel Construction Using CNC-Based Design Workflows. *American Journal of Interdisciplinary Studies*, *3*(04), 464-499. https://doi.org/10.63125/n08g1x15

[47]. Md. Mainuddin, F., & Palash Chandra, D. (2023). Advanced Computing–Based Modeling of Steel Connection Behavior and Stability Performance using ETABS And STAAD Pro. *American Journal of Advanced Technology and Engineering Solutions*, *3*(04), 42-86. https://doi.org/10.63125/xfkzrg56

[48]. Md. Mehedi, H., & Khairum Nahar, P. (2023). A Systematic Review of Secure Health Data Information Systems for Pandemic Preparedness and Economic Continuity in the United States. *Review of Applied Science and Technology*, *2*(01), 227–258. https://doi.org/10.63125/77h2m531

[49]. Md. Mehedi, H., & Khairum Nahar, P. (2024). Advanced Computing and AI-Driven National Information Systems for Predictive Disaster Risk Management and Economic Loss Mitigation. *American Journal of Scholarly Research and Innovation*, *3*(02), 296–336. https://doi.org/10.63125/4sbz5j45

[50]. Md. Morshedul, I., Rukaiya Khatun, M., & Khairum Nahar, P. (2022). Machine Learning–Driven Forecasting Pipelines for Financial Volatility Detection in Integrated Enterprise ERP Environments. *American Journal of Advanced Technology and Engineering Solutions*, *2*(02), 134-173. https://doi.org/10.63125/y42nk811

[51]. Md. Nazmul, H., & Amena Begum, S. (2022). AI-Based Psychodiagnostics' Models to Support Early Intervention and Reduce Suicide Risk in Adolescents and Youth: Development and Clinical Validation. *American Journal of Data Science and Analytics*, *3*(06), 40-79. https://doi.org/10.63125/vb5f7e98

[52]. Md. Shahinur, I., & Md. Sultan, M. (2022). Digital-Twin-Based Quantitative Frameworks for Modeling, Monitoring, and Optimization of Electrical Power Infrastructure. *American Journal of Interdisciplinary Studies*, *3*(04), 365-393. https://doi.org/10.63125/dvmj1y93

[53]. Md. Towhidul, I., & Uddin, M. D. S. (2024). Simulation-Based Forecasting and Inventory Control Models For Consumer Goods Networks: A Quantitative Study Using Monte Carlo Simulation and Time-Series Methods. *Review of Applied Science and Technology*, *3*(04), 165–197. https://doi.org/10.63125/a3047d06

[54]. Mohammad Robel, M. (2025). Advanced Computing Frameworks for Distributed Training, Deployment, and Monitoring of Artificial Intelligence and Machine Learning Models. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1922–1957. https://doi.org/10.63125/rxb2cb66

[55]. Mohammad Robel, M., & Md. Morshedul, I. (2021). Foundational Approaches to Secure Data Collection and Processing in Networked and Distributed Computing Environments. *International Journal of Business and Economics Insights*, *1*(4), 32–69. https://doi.org/10.63125/thrtkw71

[56]. Mohammad Robel, M., & Md. Morshedul, I. (2024). Data Preprocessing and Feature Engineering Strategies for Large-Scale Predictive Modeling Applications. *Review of Applied Science and Technology*, *3*(01), 263–302. https://doi.org/10.63125/tqqqed47

[57]. Mostafa, K. (2023). An Empirical Evaluation of Machine Learning Techniques for Financial Fraud Detection in Transaction-Level Data. *American Journal of Interdisciplinary Studies*, *4*(04), 210-249. https://doi.org/10.63125/60amyk26

[58]. Murad, M. D. H. R. (2025). Machine Learning–Based Consumer Behavior Prediction Models for E-Commerce Platforms: Enhancing Digital Financial Inclusion and Market Accessibility. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 2078–2118. https://doi.org/10.63125/pnz32s94

[59]. Nikkel, B. J. (2014). Fostering incident response and digital forensics research. *Digital Investigation*, *11*, 249–251. https://doi.org/10.1016/j.diin.2014.09.004

[60]. Palash Chandra, D. (2023). Machine Learning–Driven Optimization of Water Distribution Networks: Demand Forecasting, and Energy Efficiency Analysis. *Journal of Sustainable Development and Policy*, *2*(04), 257-296. https://doi.org/10.63125/jdxq0819

[61]. Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*, 816–826. https://doi.org/10.1016/j.cose.2009.05.008
[62]. Riba, J., Erkoyuncu, J., & Thobens, G. (2020). Ransomware: An empirical study of the factors that influence an organisation's decision to pay. *Journal of Cybersecurity*, *6*. https://doi.org/10.1093/cybsec/tyaa023
[63]. Rigon, E. A., Westphall, C. M., dos Santos, D. R., & Westphall, C. B. (2014). A cyclical evaluation model of information security maturity. *Information Management & Computer Security*, *22*, 265–282. https://doi.org/10.1108/imcs-04-2013-0025
[64]. Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, *30*, 256–286. https://doi.org/10.1002/pam.20567
[65]. Rosati, P., Cummins, M., Deeney, P., Gogolin, F., van der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis*, *49*, 146–154. https://doi.org/10.1016/j.irfa.2017.01.001
[66]. Rosati, P., Deeney, P., Cummins, M., van der Werff, L., & Lynn, T. (2018). Social media and stock price reaction to data breach announcements: Evidence from U.S. listed companies. *Research in International Business and Finance*, *47*, 458–469. https://doi.org/10.1016/j.ribaf.2018.09.007
[67]. Rukaiya Khatun, M., & Zakia, A. (2023). Quantitative Assessment of Data Privacy and Access Control Effectiveness in SAP/ERP Analytics Systems. *Review of Applied Science and Technology*, *2*(01), 259–300. https://doi.org/10.63125/vb03b363
[68]. Rus, I. (2015). Technologies and methods for auditing databases. *Procedia Economics and Finance*, *26*, 991–999. https://doi.org/10.1016/s2212-5671(15)00921-1
[69]. Sedayao, J., Su, S., Ma, X., Jiang, M., & Miao, K. (2009). A simple technique for securing data at rest stored in a computing cloud. In *Cloud Computing (CloudCom 2009)* (Vol. 5931, pp. 553–558). https://doi.org/10.1007/978-3-642-10665-1_51
[70]. Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*, 314–341. https://doi.org/10.1080/07421222.2015.1063315
[71]. Shaikh, S. A., & Kalutarage, H. K. (2016). Effective network security monitoring: From attribution to target-centric monitoring. *Telecommunication Systems*, *62*, 167–178. https://doi.org/10.1007/s11235-015-0071-0
[72]. Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*, 487–502. https://doi.org/10.2307/25750688
[73]. Soriano-Salvador, E., & Guardiola-Múzquiz, G. (2021). SealFS: Storage-based tamper-evident logging. *Computers & Security*, *108*, 102325. https://doi.org/10.1016/j.cose.2021.102325
[74]. Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, *58*, 216–229. https://doi.org/10.1016/j.cose.2015.12.006
[75]. Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*, 503–522. https://doi.org/10.2307/25750689
[76]. Tandon, A., Nayyar, A., & Kumar, S. (2021). Ransomware in cybersecurity: A comprehensive survey. *Computers & Security*, *111*, 102490. https://doi.org/10.1016/j.cose.2021.102490
[77]. Tanjina Binte, S., & Md. Hasan Or, R. (2022). Advanced Computing, IT Strategy, and Network-Optimized Frameworks for Retail Business Intelligence. *American Journal of Interdisciplinary Studies*, *3*(04), 429-463. https://doi.org/10.63125/dgyg3762
[78]. Tripathi, S., & Meshram, B. B. (2012). Digital evidence for database tamper detection. *Journal of Information Security*, *3*, 113–121. https://doi.org/10.4236/jis.2012.32014
[79]. Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*, 190–198. https://doi.org/10.1016/j.im.2012.04.002
[80]. Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*, 576–586. https://doi.org/10.1016/j.dss.2011.03.002
[81]. Vishwanath, A., Neo, L. S., Goh, Q. Y., Lee, S. H., & Ong, R. (2020). Cyber hygiene: The concept, its measure, and initial tests. *Decision Support Systems*, *128*, 113160. https://doi.org/10.1016/j.dss.2019.113160
[82]. Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly*, *39*, 91–112. https://doi.org/10.25300/misq/2015/39.1.05
[83]. Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*, 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005
[84]. Xie, S. L. (2019). A must for agencies or a candidate for deletion: A grounded theory investigation of the relationships between records management and information security. *Records Management Journal*, *29*, 57–85. https://doi.org/10.1108/rmj-09-2018-0026
[85]. Yeh, Q.-J., & Chang, A. J.-T. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management*, *44*, 480–491. https://doi.org/10.1016/j.im.2007.05.003
[86]. Zakia, A., & Rukaiya Khatun, M. (2024). Quantitative Assessment of CRM-Based Business Intelligence on Customer Satisfaction and Retention: Evidence from Multi-Channel Service Operations. *Journal of Sustainable Development and Policy*, *3*(02), 01-42. https://doi.org/10.63125/hjd22x72