INTERNATIONAL JOURNAL OF BUSINESS AND ECONOMICS INSIGHTS

Volume: 5; **Issue:** 3
Pages: 459– 493
Accepted: 29 August 2025
Published: 07 October 2025

SECURING ERP SYSTEMS: THE ROLE OF INFORMATION SECURITY ANALYSTS IN U.S. TEXTILE AND MANUFACTURING ENTERPRISES

Zamal Haider Shish[1]

[1]. *Master of Science in Instructional Design and Technology, Department of Education, The University of Tampa, USA; Email: hsjidan@gmail.com*

Doi: 10.63125/y8evt228
This work was peer-reviewed under the editorial responsibility of the IJEI, 2025

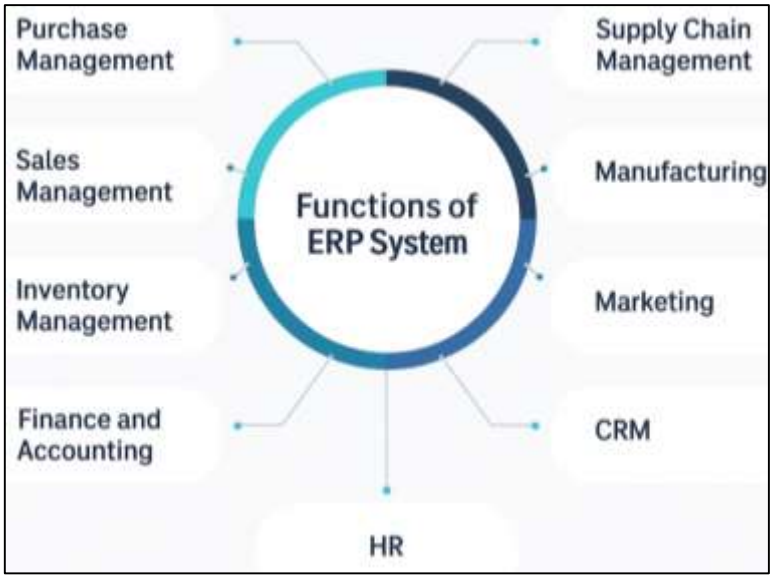
Abstract
This study addresses a persistent problem in U.S. textile and manufacturing enterprises: Enterprise Resource Planning environments are integral to operations yet remain vulnerable, and there is limited sector-specific, quantitative evidence on how information security analysts shape ERP security effectiveness. The purpose is to quantify the associations between analyst-centered capabilities and measurable ERP security outcomes. Design is quantitative, cross-sectional, and multi-case. The sample comprises N = 178 firm-level cases spanning cloud, on-premises, and hybrid ERP deployments. The literature review informing the framework synthesized 44 peer-reviewed sources. Key variables include an outcome composite for ERP security effectiveness incident frequency, severity, time to recover, segregation-of-duties posture, and audit signals, and focal predictors for analyst competency, staffing adequacy, and practice maturity, with security culture as a mediator and deployment model as a moderator. The analysis plan specified descriptive statistics, reliability checks, correlations, and multiple regression with heteroskedasticity-robust errors, plus mediation via bootstrap and moderation by cloud, with robustness checks using negative binomial for incident counts, ordinal logit for severity, and log-linear models for recovery time. Headline findings show analyst competency and practice maturity as the strongest unique predictors of effectiveness standardized $\beta \approx 0.28$ and 0.31, adjusted $R^2 \approx 0.46$, staffing adequacy is positive but smaller, security culture partially mediates these relationships, and the competency effect is steeper among cloud adopters; incident counts and recovery time improve materially incidence-rate ratios around 0.79 to 0.75 and 11 to 13 percent faster recovery per one-point increase on five-point scales. Implications are to prioritize ERP-specific IAM and SoD engineering, cadence-driven practice maturity, ERP-aware monitoring, and culture building, and to leverage cloud platform affordances to amplify competency gains.

Keywords
ERP Security; Information Security Analysts; Textile Manufacturing; Cloud ERP; Segregation Of Duties; Role-Based Access Control; Practice Maturity;

INTRODUCTION

Enterprise Resource Planning (ERP) systems represent comprehensive, integrated suites of software modules designed to centralize, streamline, and automate an organization's core business processes ranging from finance, procurement, and production planning to inventory management, sales, and human resources within a unified data architecture (Chang et al., 2014). In the modern manufacturing landscape, ERPs serve as the digital and transactional backbone that seamlessly links the "shop floor" to the "top floor," harmonizing data exchange between operational technology (OT) and information technology (IT) domains to ensure synchronized decision-making and process visibility (Wu et al., 2018). From an information-assurance perspective, ERP security entails safeguarding the confidentiality, integrity, and availability (CIA) of the diverse assets data, user identities, workflows, and system interfaces that the ERP environment orchestrates (Kankanhalli et al., 2003). Given that ERP platforms mediate high-stakes processes such as procure-to-pay and order-to-cash, any breach of CIA whether through unauthorized access, misconfigurations, privilege escalation, or breakdowns in inter-system trust can cascade across departments and production sites, causing widespread operational disruptions (Bradford et al., 2014; Chang et al., 2014). This interconnectedness renders ERP ecosystems both indispensable and inherently vulnerable, particularly in manufacturing and textile industries characterized by intricate supply chains, razor-thin profit margins, and just-in-time production demands, where any compromise in data assurance can directly translate into financial loss and reputational damage (Wu et al., 2018). Therefore, securing ERP systems transcends mere technical safeguards; it embodies a holistic enterprise risk management imperative that integrates strategic governance with proactive oversight. Accordingly, the present study conceptualizes ERP security as the synergistic ensemble of technological controls, organizational governance frameworks, and continuous monitoring practices that collectively protect identities, roles, data flows, and inter-application integrations, thereby mitigating risks of misuse, error, and compromise within ERP-mediated business operations (Chang et al., 2014; Colantonio et al., 2009).

Figure 1: Overview of ERP System



The global body of research highlights two interrelated and compelling rationales for prioritizing ERP security within manufacturing enterprises: the concentration of critical business logic and the accelerating digitization of production environments. ERPs serve as the central nervous system of industrial organizations by consolidating authorizations, workflows, and process logic into a unified platform. While this integration enables operational efficiency and economies of scale, it simultaneously amplifies potential vulnerabilities by expanding the scope of damage should access controls or governance mechanisms fail (Bradford et al., 2014). Empirical evidence underscores that weaknesses in ERP control domains particularly those related to change management, segregation of

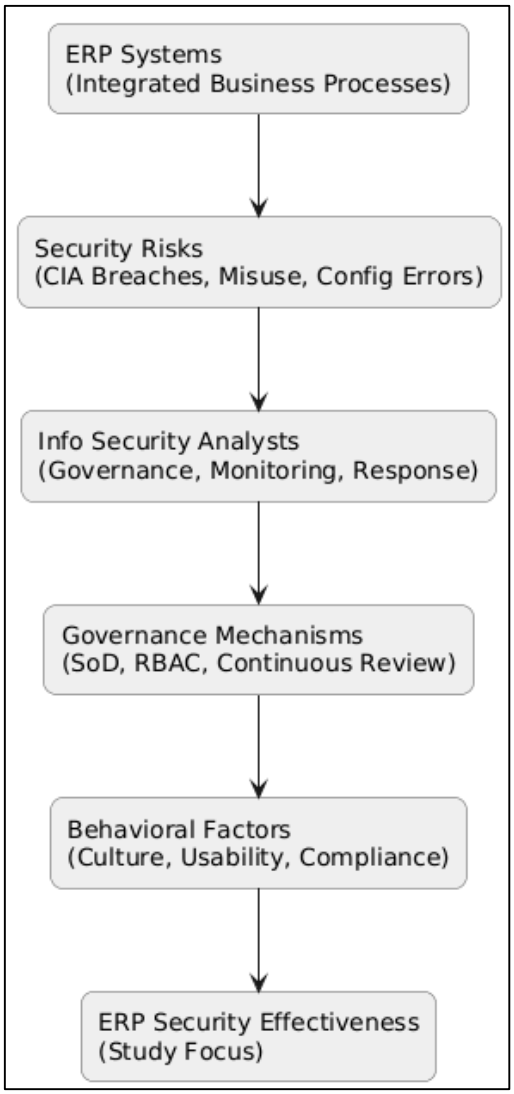
duties (SoD), and role design are systematically linked to audit irregularities, compliance breaches, and process inefficiencies, reinforcing the necessity of robust ERP governance structures (Bradford et al., 2014; Chang et al., 2014; Ferraiolo et al., 2001). Complementing this structural concentration of logic is the rapid digital transformation of manufacturing through technologies such as the Industrial Internet of Things (IIoT), computer-integrated manufacturing, and additive manufacturing, which together forge a tightly coupled ecosystem where ERP transactions directly influence operational technology (OT) events. This growing interdependence creates a proliferation of interfaces and, consequently, an expansion of potential attack surfaces that adversaries may exploit (Johnston & Warkentin, 2010). Scholarly reviews on digital manufacturing security consistently reveal that vulnerabilities often arise at the junctions linking design repositories, manufacturing execution systems (MES), supervisory control and data acquisition (SCADA) networks, and enterprise IT systems. These studies note that issues related to identity management, authorization, and data integrity commonly originate from upstream business applications most notably the ERP platform itself (Johnston & Warkentin, 2010). Together, these intertwined dynamics substantiate the urgent need to strengthen the empirical foundation connecting ERP security practices with tangible, quantifiable reductions in cybersecurity and operational risks across the manufacturing landscape.

Within this intricate risk environment, information security analysts serve as the first line of operational defense, translating organizational security strategies into concrete, actionable safeguards. As defined in this study, their responsibilities encompass evaluating threats and controls across ERP modules, designing and maintaining segregation of duties (SoD) and role-based access control (RBAC) architectures, monitoring anomalies in user identities and data flows, and orchestrating responses when incidents arise within ERP ecosystems (Bulgurcu et al., 2010; Rezaul, 2021). Their effectiveness, however, does not exist in isolation; it is profoundly shaped by the surrounding control environment, including organizational policies, management support, and the overall culture of security awareness, as well as by end users' behavioral responses to established controls (Liang & Xue, 2010; Ismail, 2022; Safa et al., 2015). Research in organizational and behavioral security underscores that even the most technically sound controls can falter if they are misaligned with user behavior or operational workflows. Hence, analysts must not only ensure technical robustness but also engineer controls that are intuitive and usable crafting business-relevant roles that avoid toxic permission overlaps and reduce the temptation for unauthorized shortcuts or risky workarounds (Hossen & Atiqur, 2022; Posey et al., 2013). In manufacturing and textile enterprises, where ERP systems integrate core production, supply chain, and financial processes, the analyst's capacity to maintain this delicate balance between security rigor and operational usability becomes especially critical. Accordingly, this study situates analysts' practices in access governance, anomaly monitoring, and incident coordination as central determinants of ERP security performance, positing that the quality and usability of their interventions directly influence the resilience and risk posture of enterprise systems in digitally intensive manufacturing contexts.

Access governance stands at the heart of ERP security because it directly regulates who can do what within the system, determining the integrity of financial, operational, and compliance outcomes. Over-privileged accounts and conflicting entitlements are repeatedly identified as major precursors to fraud, process manipulation, and sensitive data exposure, underscoring the importance of disciplined access control frameworks (Razia, 2022). The principle of segregation of duties (SoD) is central to this governance, as it deliberately allocates critical permissions across multiple users to ensure that no single individual can independently initiate, authorize, and complete high-risk transactions. When SoD frameworks are inadequately designed or inconsistently maintained, organizations face latent risks that allow undetected errors or deliberate misconduct to propagate through enterprise processes (Herath & Rao, 2009; Sadia, 2022). Complementary to SoD, role-based access control (RBAC) provides the structural mechanism for translating business responsibilities into defined role templates. When RBAC structures are aligned with actual operational tasks, constraints, and accountability chains, organizations achieve both stronger compliance and greater efficiency, as evidenced by reduced violations and less rework during audit cycles (Ifinedo, 2014; Arif Uz & Elmoon, 2023). The broader body of empirical and design science research consistently stresses that access governance in ERP

systems is not a one-time configuration but a dynamic process requiring continuous refinement. Authorizations must be regularly reviewed, mined for anomalies, and refactored to keep pace with evolving business processes, reorganizations, mergers, and technological integrations (D'Arcy et al., 2009; Hasan, 2023). Within this adaptive cycle, information security analysts play a pivotal role by transforming control objectives into detailed SoD matrices, monitoring exception queues, and ensuring that every adjustment remains grounded in business logic and regulatory standards. This study therefore evaluates how analysts' execution of these governance activities contributes to measurable improvements in ERP security, using both descriptive and inferential statistical analyses to capture the depth of their impact.

Figure 1: ERP Security Effectiveness



The organizational behavior literature provides a robust explanatory lens for understanding why controls implemented by analysts endure and how human factors mediate their effectiveness (Shoeb & Reduanul, 2023). Theories grounded in protection motivation and social influence suggest that employees' adherence to security policies is shaped by perceptions of response efficacy, self-efficacy, and normative pressures, highlighting the behavioral dimension of technical controls (Vance et al., 2012; Zhang & Xu, 2016). When analysts engineer controls that are intuitive, minimize operational friction, and clearly communicate the rationale behind entitlements and role assignments, alignment with organizational policy improves, thereby reducing instances of policy circumvention, privilege creep, and ad hoc workarounds (Razia, 2023; Wang & Li, 2010). In ERP contexts, where end users operate across finance, procurement, production, and logistics functions, the usability of roles,

approval workflows, and access protocols directly influences both compliance and operational throughput. Controls that are technically sound but difficult to navigate risk non-adherence, whereas well-designed, user-centric governance mechanisms enhance both security posture and business efficiency (Reduanul, 2023). Building on these insights, this study positions analyst capabilities encompassing access design, monitoring, and incident management as critical determinants of ERP security outcomes. The research framework links these technical competencies with observable ERP security metrics while the survey instruments simultaneously capture behavioral responses to controls, grounding the analysis in established constructs from the organizational behavior and information security literature (Alasmary et al., 2020; Sandhu et al., 1996). This dual technical-behavioral perspective allows for a comprehensive assessment of how human factors, policy design, and analyst expertise collectively shape the resilience of ERP systems in complex, multi-functional enterprise environments. This study ultimately frames ERP security as a socio-technical capability that carries strategic importance for manufacturing performance, moving beyond the view of controls as mere constraints (Sadia, 2023). By positioning ERP security mechanisms as enablers of operational reliability, analysts help safeguard data integrity across planning, costing, and supplier collaboration processes foundational elements for maintaining competitive agility in textile and manufacturing enterprises (Ahn & Sandhu, 2000; Ismail, 2024). Methodologically, the research employs a cross-sectional, multi–case design, capturing both analyst practices and ERP security outcomes through Likert-scale survey instruments and objective audit and monitoring indicators. Relationships between analyst activities and system security are examined using correlation and regression techniques, allowing for nuanced insights into the operational impact of security governance (Mesbaul, 2024). The analysis focuses on three interconnected control domains: identity and access governance with segregation of duties, data integrity monitoring, and coordination of incident response. By integrating these domains, the study situates the work of information security analysts within the real-world production and supply chain processes that ERP systems enable, illustrating how their expertise in access design, anomaly detection, and response orchestration translates into measurable improvements in compliance, risk reduction, and overall system resilience (Omar, 2024; Siponen & Vance, 2010).

The objective of this study is to produce rigorous, sector-specific, quantitative evidence on how information security analysts shape the security effectiveness of Enterprise Resource Planning environments in U.S. textile and manufacturing enterprises. First, the study will develop and administer a structured Likert-scale instrument to measure four constructs: ERP security effectiveness (incident frequency, mean severity, time to recovery, segregation-of-duties violations, and audit findings), analyst competency (ERP access governance expertise, incident response capability, monitoring and analytics proficiency, and domain experience), staffing adequacy (coverage ratios, workload backlogs, and support hours), and practice maturity (patch cadence, change-management discipline, logging and alerting coverage, and access-review frequency). Second, the study will describe the current ERP security posture across cases by reporting comprehensive descriptive statistics and construct reliability results, thereby establishing an empirical baseline for the sector. Third, the study will test a set of theoretically grounded hypotheses using correlation and multiple regression models to estimate the unique and combined contributions of analyst competency, staffing, and practice maturity to observed security outcomes while controlling for organizational size, ERP deployment model, vendor, subsector, and level of OT/IT integration. Fourth, the study will evaluate a mediation pathway in which security culture functions as a mechanism linking analyst factors to security effectiveness, and will probe a moderation effect that compares the strength of analyst-related impacts in cloud versus on-premises ERP deployments. Fifth, the study will generate practical benchmarks by deriving recommended staffing ratios and competency profiles associated with favorable outcome bands, alongside sensitivity and robustness checks that reestimate models for alternative outcome codings and exclude influential observations. Sixth, the study will produce a transparent codebook, scoring guide, and analysis specification that enable replication and reuse by practitioners and researchers.

LITERATURE REVIEW

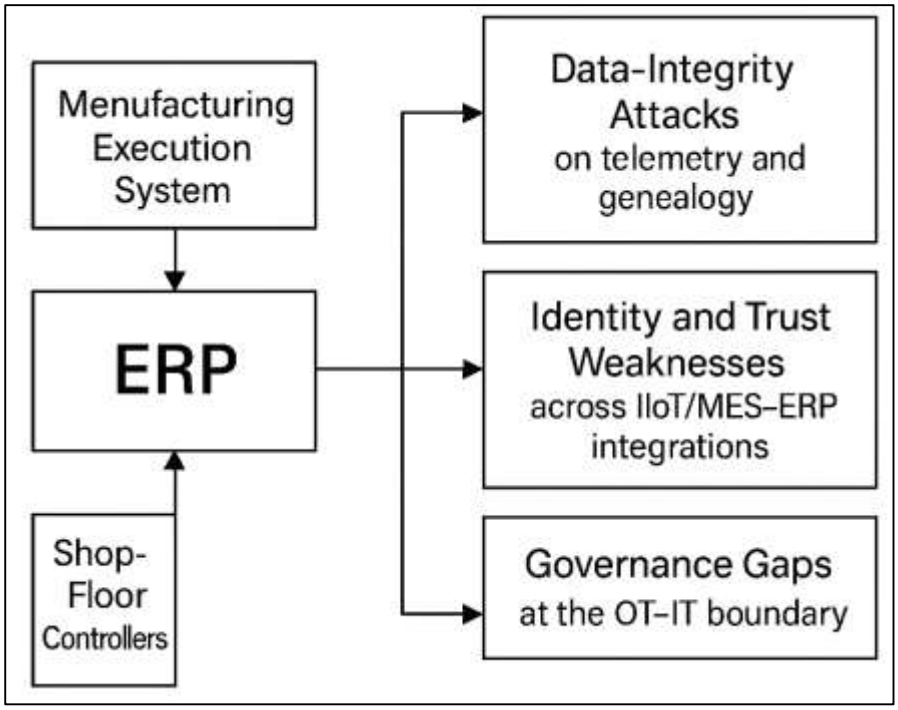
The literature on securing Enterprise Resource Planning (ERP) systems in manufacturing presents a converging yet still fragmented body of evidence that spans technical controls, governance frameworks, and human factors, with particular salience for sectors such as textiles where high product mix, supplier variability, and thin margins amplify operational risk. Foundational streams position ERP as the transactional backbone linking finance, procurement, production planning, and logistics to plant-level execution, making identity and access governance, segregation of duties, change management, and continuous monitoring the primary levers for preserving data integrity and process continuity. Building on this base, research in role engineering and SoD analytics demonstrates that control quality depends not only on formal policies but also on the semantic fit between roles and real business tasks, a fit that drifts as organizations reconfigure workflows, integrate partners, or shift from on-premises to cloud ERP models (Rezaul & Hossen, 2024). Parallel work in manufacturing cybersecurity highlights the growing interface density among ERP, MES/SCADA, PLM, and supplier platforms, expanding the attack surface and transferring a portion of OT risk upstream into business applications, including authorization design and inter-system trust (Momena & Sai Praveen, 2024). Behavioral and organizational studies add mechanism-rich explanations for why controls succeed or fail in practice: security culture, managerial support, analyst communication, and perceived usability of workflows shape end-user compliance, privilege creep, and the frequency of policy workarounds. Within this multi-disciplinary landscape, the role of information security analysts emerges as an operational fulcrum translating governance intent into workable access models, maintaining monitoring coverage and signal quality, coordinating incident response, and stewarding remediation cycles that align with production constraints. Yet, despite robust conceptual models and case illustrations, quantitative, sector-specific evidence linking analyst competencies, staffing adequacy, and practice maturity to measurable ERP security outcomes remains comparatively sparse, especially for U.S. textile and manufacturing enterprises (Muhammad, 2024). This review therefore synthesizes four interlocking domains ERP security risks and controls in manufacturing contexts; analyst roles and competencies in ERP environments; governance and standards that structure ERP control systems; and theoretical perspectives that explain adoption, compliance, and control effectiveness to identify validated constructs, measurement strategies, and empirical gaps that motivate the present study's research questions and hypotheses.

ERP-Adjacent Security Risks

Manufacturing and textile enterprises increasingly digitize core operations by integrating enterprise resource planning (ERP) with manufacturing execution systems (MES), shop-floor controllers, and the industrial internet of things (IIoT). This IT–OT convergence transforms ERP from a back-office ledger into a live orchestration hub that exchanges credentials, master data, and production instructions with cyber-physical assets thereby inheriting their risk surface (Noor et al., 2024). In tightly coupled environments, integrity loss at the edge (e.g., tampered sensor readings, spoofed machine states) can propagate upstream as corrupted work orders, bills of materials, or inventory positions that ERP then "legitimizes" across finance, procurement, and logistics. At the architectural level, IIoT expansion broadens identity sprawl, multiplies machine-to-machine trust links, and complicates network zoning; these dynamics are well documented in analyses of IIoT threat exposure in industrial settings and directly map to ERP integration endpoints (APIs, message buses, and brokers) that bridge corporate networks and production cells (Abdul, 2025; Boyes et al., 2018). Likewise, cyber-physical systems (CPS) surveys show that cross-domain attacks exploit feedback loops between software and physical processes; when ERP participates in those loops (e.g., automated quality holds, maintenance triggers), adversaries can weaponize "business-as-code" by manipulating upstream signals to cause erroneous ERP decisions with real economic impact (Elmoon, 2025a; Humayed et al., 2017). These risks are accentuated in textiles, where batch variability, rapid style changes, and outsourced finishing create frequent ERP updates and partner connectivity expanding the blast radius of compromised data flows. In short, ERP in manufacturing is no longer insulated from operational threats; it is a high-value nexus through which CPS/IIoT compromises can be monetized at enterprise scale (Boyes et al., 2018; Elmoon, 2025b; Humayed et al., 2017).

Once ERP becomes part of an extended CPS, classic industrial control system (ICS) shortcomings legacy protocols, flat networks, weak authentication on controllers, and limited patch windows materially degrade the effectiveness of enterprise-grade controls such as role-based access and workflow approvals (Hozyfa, 2025). Empirical reviews of ICS security management report persistent gaps in risk assessment practices tailored to plant realities (availability-first, safety-critical constraints), limited security metrics, and challenges coordinating responsibilities across operations and IT; these governance fissures undermine end-to-end assurance and create blind spots where ERP trusts upstream records or commands without independent validation (Alam, 2025; Knowles et al., 2015). From a vulnerability standpoint, smart-manufacturing literature chronicles concrete failure modes: spoofing of metrology data that silently biases quality decisions; man-in-the-middle attacks on field-to-MES links that alter production counts or genealogy; malicious firmware that drifts process parameters; and lateral movement from third-party maintenance access into production networks all of which can trigger inaccurate ERP postings (e.g., false scrap, phantom WIP, misstated yields) that cascade into planning, costing, and revenue recognition (Masud, 2025; Tuptuk & Hailes, 2018). Because ERP modules often automate tolerances, release thresholds, or vendor returns based on telemetry, adversaries need not breach ERP directly; corrupting trusted inputs can coerce ERP to enact harmful business outcomes while leaving few traditional application-security indicators. Moreover, textiles' seasonal demand and contract manufacturing magnify dependencies on inter-organizational data exchange (EDI, supplier portals, cloud MES). As IIoT frameworks emphasize, every new device class and gateway expands the identity, certificate, and key-management burden, raising the odds of misconfiguration that exposes ERP integration middleware or message queues (Boyes et al., 2018; Mrman, 2025; Tuptuk & Hailes, 2018). The operational tempo short changeovers, 24/7 lines also constrains patching windows, forcing compensating controls and heightening the importance of detection at the business-process layer (Knowles et al., 2015; Mohaiminul, 2025).

Figure 2: ERP-adjacent security risks in U.S. manufacturing and textile enterprises



In addition, research focused specifically on manufacturing cyber-physical threats highlights the ways adversaries exploit production semantics that traditional IT defenses overlook. Short communications in Manufacturing Letters outlined how integrity attacks that minimally perturb toolpaths, set-points, or inspection thresholds can pass network-centric defenses yet degrade product conformance and safety, all while the ERP system dutifully records plausible transactions and variances (Mominul, 2025; Wells et al., 2014). CPS surveys reinforce those successful attacks often chain modest weaknesses (e.g.,

weak device onboarding, default credentials on HMIs, insufficient segmentation around brokers) into business-level consequences, suggesting ERP risk assessments must span beyond app-tier controls to include plant-floor trust boundaries and message integrity guarantees (Humayed et al., 2017; Wells et al., 2014). When mapped to textile manufacturing, such attack paths are particularly pernicious: cut-and-sew lines depend on accurate nesting and consumption factors; dyeing/finishing relies on precise recipes and dwell times; and compliance (e.g., fiber content, country-of-origin) depends on genealogy integrity (Rezaul, 2025). If an attacker tampers with counters or recipe parameters at the CPS layer, ERP may propagate false material usage, non-compliant labeling, or misstated labor standards exposing firms to chargebacks, recalls, or sanctions. The literature therefore implies three salient ERP-adjacent risk clusters for U.S. manufacturers and textile enterprises: (1) data-integrity attacks on telemetry and genealogy that subvert ERP's "system-of-record" role; (2) identity and trust weaknesses across IIoT/MES–ERP integrations that enable privilege escalation and command abuse; and (3) governance gaps at the OT–IT boundary that leave ERP workflows vulnerable to high-impact, low-visibility manipulations (Humayed et al., 2017; Tuptuk & Hailes, 2018; Wells et al., 2014). Addressing these clusters requires aligning ERP security assumptions with CPS realities treating integrity at the edge as a prerequisite for trustworthy enterprise decisions rather than an afterthought confined to the plant network perimeter (Knowles et al., 2015; Rezaul & Rony, 2025).

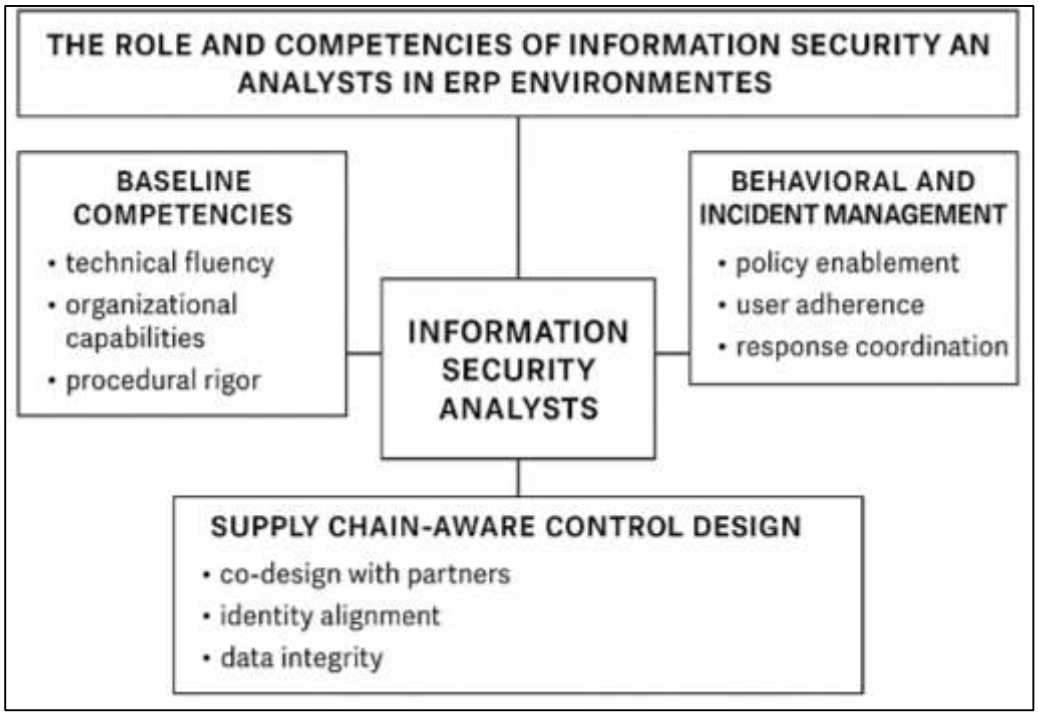
Information Security Analysts in ERP Environments

In ERP-intensive enterprises, information security analysts (ISAs) act as the connective tissue that translates high-level governance into daily, auditable controls spanning identity, data, and process integrity. The baseline competence profile blends technical fluency (e.g., access-control models, logging and detection engineering, secure integration patterns) with organizational capabilities (stakeholder alignment, change enablement, risk communication) and procedural rigor (policy operationalization, incident runbooks, post-incident learning). Three workstreams are particularly salient around ERP: (1) access governance and authorization engineering; (2) monitoring, detection, and incident response across application–integration layers; and (3) control assurance embedded in supply-chain–facing processes. On the authorization front, analysts must be sufficiently conversant with both role/attribute-based access models to design entitlements that reflect business semantics (role hierarchies, separation-of-duties constraints, exception workflows) without creating toxic permission combinations that elevate fraud or error exposure. On monitoring and response, analysts curate ERP-aware signals (privilege escalations, cross-module anomalies, unusual SoD override patterns), enrich events with business context, and drive triage that balances availability and integrity for time-sensitive operations. Organizationally, the job requires negotiating trade-offs with finance, procurement, production planning, and vendor-management teams so that controls remain usable, explainable, and resilient under peak loads and cutover windows (Hasan, 2025). The literature on incident management underscores how analysts' competencies must span pre-breach preparedness, coordinated response, and continuous improvement; without that end-to-end discipline, even well-designed ERP controls can degrade in the face of evolving workflows and partner integrations (Milon, 2025; Tøndel et al., 2014). Similarly, studies of security management practice show that analysts' effectiveness is bounded not only by tooling but by human and organizational frictions ambiguities in responsibility, limited domain knowledge on the business side, and gaps in feedback loops between security and operations making communication, boundary spanning, and sensemaking first-order analyst skills in ERP contexts (Rabiul, 2025; Werlinger et al., 2009).

Translating access-control theory into ERP reality is a distinctive analyst competency because ERP authorizations encode business logic and compliance duties. Beyond classic role-based access control (RBAC), modern ERP landscapes frequently require attribute-based access control (ABAC) patterns to capture context (plant, cost center, project, vendor tier, material class) and dynamic constraints (order value thresholds, period close windows) (Hasan & Abdul, 2025). Analysts therefore need modeling skills to choose and combine RBAC/ABAC mechanisms, manage delegation, and specify policy conflict resolution in ways that remain maintainable at enterprise scale (Farabe, 2025). Research on unified ABAC for enterprise systems clarifies how attributes, policy combining algorithms, and obligation handling can be structured to reflect real organizational rules while supporting auditability and change control capabilities that ISAs must internalize to avoid brittle, exception-ridden designs

(Jin et al., 2012; Momena, 2025). Yet authorization engineering is only half the task; ERP value chains extend into suppliers, logistics providers, and contract manufacturers. Embedding security into supply-chain processes purchase-to-pay, vendor onboarding, advance ship notice reconciliation requires analysts to co-design controls that ensure data provenance, gate risky transactions, and align identity lifecycles across organizational boundaries. Empirical work on integrating information security into supply-chain management stresses that analysts must anticipate and mitigate cross-firm trust gaps (e.g., credential reuse, inconsistent vetting, weak partner monitoring) because those gaps routinely become the attack paths that later surface as ERP anomalies (Johnson & Goetz, 2007; Mubashir, 2025). In practice, that means ISAs articulate minimum control baselines for partner connectivity (certificate handling, message integrity, least-privilege service accounts) and operationalize verification (attestation evidence, exception reporting), thereby keeping ERP's "system-of-record" status credible across the wider ecosystem.

Figure 3: The role and competencies of information security analysts in ERP environments



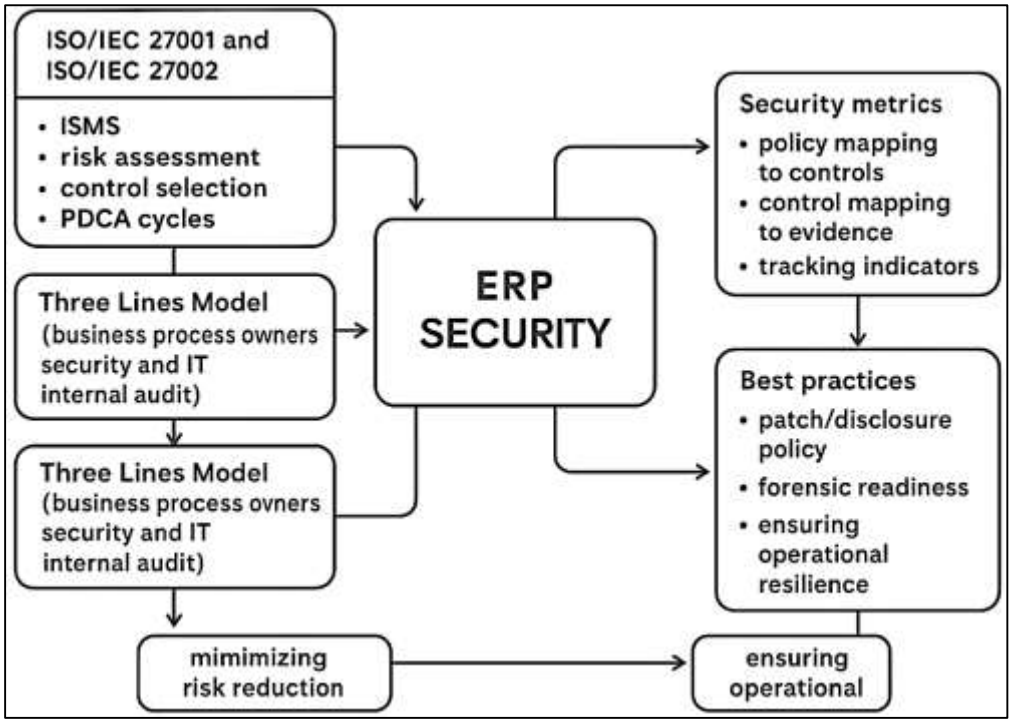
Because ERP programs reshape everyday work for large, heterogeneous user populations, analysts must also master the behavioral side of control adoption: how users perceive, learn, and enact policies in the flow of work (Pankaz Roy, 2025). Competence here extends beyond "awareness" to the design of interventions that build self-efficacy, minimize friction, and cultivate internalized norms of secure behavior within finance, operations, and plant teams (Rahman, 2025). Controlled studies on security training and compliance demonstrate that instructional design choices and contextualization profoundly influence whether policies are enacted or bypassed; effective programs tailor content to roles, use problem-centered scenarios, and reinforce desired behaviors with timely feedback rather than generic, compliance-only messaging (Puhakainen & Siponen, 2010; Rakibul, 2025). Complementary evidence from practice analyses shows that security management succeeds when analysts orchestrate the human, organizational, and technological facets as a coherent system aligning incentives, clarifying accountability, and iterating controls with business input (Reduanul, 2025; Werlinger et al., 2009). Finally, incident-management competence closes the loop: in complex ERP ecosystems, analysts must coordinate multi-party responses (internal teams, vendors, partners), maintain decision logs, and drive after-action learning that hardens both preventive and detective controls (Rony, 2025). Reviews of incident management highlight the importance of readiness (playbooks, roles, communication channels), structured containment and eradication, and metrics that track remediation quality not just

speed so that ERP change management, access reviews, and monitoring rules mature after each event (Saba, 2025; Werlinger et al., 2009). When these competencies are present authorization engineering that reflects business semantics, supply-chain-aware control design, behaviorally informed policy enablement, and life-cycle incident management ISAs become the operational fulcrum that sustains ERP security without undermining throughput or agility (Jin et al., 2012; Johnson & Goetz, 2007).

Governance to ERP Security

As enterprise resource planning (ERP) platforms have become the transactional backbone of manufacturing, governance frameworks and security standards provide the scaffolding for translating high-level objectives into auditable, day-to-day controls. ISO/IEC 27001 and ISO/IEC 27002 are especially important because they formalize an information security management system (ISMS) that spans policy, risk assessment, control selection, and continuous improvement elements that map directly to ERP domains such as identity and access governance, change and release management, supplier connectivity, and logging/monitoring (Kumar, 2025). In textile and discrete manufacturing environments, an ISO-aligned ISMS anchors the "three lines" model: business process owners define control objectives (e.g., segregation of duties and least privilege), security and IT operationalize them in role designs, integration gateways, and monitoring rules, and internal audit assures their effectiveness through evidence trails. For ERP, the practical value of ISO/IEC 27001 lies in its cadence: regular risk assessments drive updates to authorization matrices, interface whitelists, and patch windows (Praveen, 2025); Plan-Do-Check-Act (PDCA) cycles institutionalize post-incident learning into change controls and exception handling; and Annex A control families (e.g., access control, operations security, supplier relationships, and information transfer) offer traceable line-of-sight from risk to control to test. This governance posture is not purely symbolic; it gives plant-constrained operations a common language for negotiating trade-offs among availability, integrity, and compliance, while creating the evidentiary artifacts risk registers, SoD rulebooks, job/role catalogs, and monitoring baselines needed to withstand regulatory scrutiny and third-party audits in supply-chain-dense sectors. In short, ISO/IEC 27001/27002 become the "spine" around which ERP security practices are prioritized, resourced, and measured in real factories with real downtime costs (Disterer, 2013; Shaikat, 2025).

Figure 4: Governance, standards, and best practices relevant to ERP security



Standards, however, are not self-executing, and experience shows that organizations frequently "implement the binder" rather than the control system. A critical body of work cautions that security management standards can devolve into compliance theater if they are transplanted without tailoring to organizational context, workflow semantics, and real decision rights (Zaki, 2025). The challenge is especially acute in ERP, where authorizations encode business logic and where small misfits overbroad roles, poorly defined SoD conflicts, ad hoc exceptions create latent pathways for fraud or operational error. The remedy is disciplined contextualization and measurement: governance should require that each policy maps to enforceable ERP controls (e.g., role hierarchies, approval chains, interface allowlists), each control maps to testable evidence (e.g., automated SoD scans, change tickets, log analytics), and each test rolls into metrics that leaders actually review and act upon (Kanti, 2025). A mature metrics program closes the loop: instead of tallying only policy adoption, firms track leading and lagging indicators such as time-to-revoke after job changes, percentage of high-risk SoD conflicts resolved per close cycle, proportion of high-severity ERP patches deployed within vendor windows, and detection coverage over critical transactions and interfaces. Systematic surveys of security metrics underline that meaningful measures require clear operational definitions, repeatable collection, and decision relevance; they should help prioritize risk reduction, not merely document activity (Zobayer, 2025). In manufacturing ERPs, that means instrumenting business-meaningful signals (e.g., unusual vendor-master edits, off-hours release of work orders, anomalous interface payloads) and using them to govern change and access rather than relying on generic counts. Put differently, standards supply the "what," but robust metrics and governance supply the "so what," ensuring that ERP security is managed as a performance system rather than a paperwork exercise (Ab Rahman et al., 2019; Siponen & Willison, 2009).

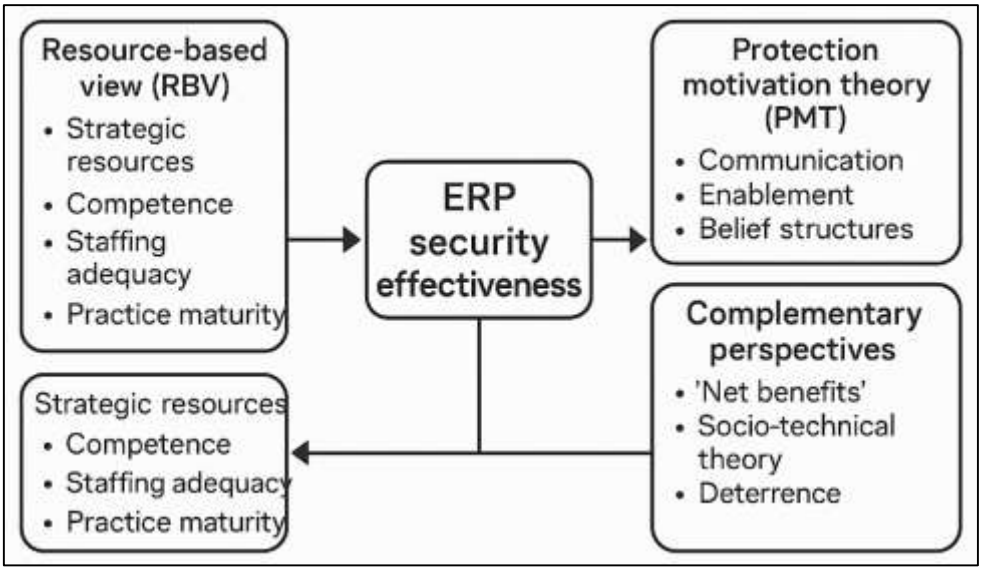
Best practice in ERP security governance also depends on how organizations manage two high-leverage control planes: (1) patch/disclosure policy that constrains exposure windows for known vulnerabilities across ERP cores, plugins, and integration middleware; and (2) forensic readiness that ensures incidents yield usable evidence spanning cloud and on-prem components (Arora et al., 2008). Economic models of vulnerability disclosure and patch timing demonstrate that policy choices influence vendor and operator behavior, thereby altering real risk: shrinking protected periods and aligning release cadences can accelerate remediation, but only if enterprises have governance that translates policy into workable maintenance windows, rollback criteria, and exception approvals aligned with plant schedules. In practice, ERP programs should make patch governance a board-visible KPI: track median days to deploy security fixes in the ERP stack and message brokers; couple emergency fixes with post-hoc change reviews; and require risk sign-offs when deferrals exceed thresholds. Equally, modern ERP estates are hybrid; forensic readiness well-designed logging, time synchronization, evidence preservation, and role-based access to logs must be engineered in advance so that cross-boundary investigations (ERP ↔ MES/PLM ↔ cloud services) can establish provenance, causality, and scope without guesswork. Empirical frameworks for cloud forensic readiness outline organizational, legal, and technical factors that materially affect this capability, from SLA clauses and multi-jurisdictional awareness to log schema, retention, and integrity protections; for ERP governance, adopting such frameworks means specifying "must-capture" events at the business-process layer (e.g., SoD overrides, payment releases, role grants), mapping them to immutable storage, and testing retrieval workflows during exercises not for the first time during a breach (Pendleton et al., 2016). Together, disciplined patch/disclosure governance and engineered forensic readiness convert standards into operational resilience, ensuring that when controls fail (as they sometimes will), exposure windows are short, root causes are knowable, and lessons learned are promptly folded back into ERP change, access, and monitoring baselines (Arora et al., 2008).

Theoretical Foundations and Empirical Gaps

A coherent theoretical footing is essential for explaining why some ERP security programs in manufacturing outperform others, even when they appear to deploy comparable controls. The resource-based view (RBV) offers a first anchor: it posits that firm-specific, valuable, rare, inimitable, and non-substitutable resources especially bundles of know-how embedded in people and routines are the engine of sustained performance differences. Applied to ERP security, RBV reframes information security analysts' competencies, the maturity of access-governance routines, and the quality of incident

response as strategic resources rather than generic IT hygiene (Barney, 1991). In plants where analysts can translate process semantics into robust SoD rule sets, maintain high-signal monitoring, and coordinate cross-functional remediation without disrupting throughput, those capabilities meet the RBV criteria and should predict superior outcomes fewer incidents, faster recovery, tighter audit performance even when technology stacks look similar across firms. This lens also clarifies why "checklist compliance" fails to equalize results: codified standards are replicable, but the situated knowledge required to operationalize ERP controls under textile/manufacturing constraints is not. RBV therefore motivates the construct choices in this study (competence, staffing adequacy, practice maturity) and the expectation that they will explain variance in measured security effectiveness above and beyond vendor, ERP model, or firm size. By grounding our hypotheses in RBV, we treat ERP security posture as a function of socio-technical capabilities that accumulate through learning and are difficult for rivals to copy simply by purchasing tools or adopting templated policies (Barney, 1991).

Figure 5: Theoretical foundations and empirical gaps informing ERP security effectiveness



A second anchor comes from cognition- and motivation-based theories of protective behavior, particularly Protection Motivation Theory (PMT). PMT explains policy-consistent action as a function of appraisals of threat severity and vulnerability, coupled with beliefs about response efficacy and self-efficacy. In ERP contexts, analysts influence all four levers: they shape perceived severity/vulnerability by communicating business-meaningful risks (e.g., toxic permission paths that enable solo-fraud in procure-to-pay); they raise response efficacy by engineering controls that demonstrably block risky actions; and they cultivate self-efficacy by training users and super-users to enact secure workflows without undue friction. When PMT is embedded into routine governance role design workshops framed around real fraud paths, change-control rationales expressed in operational terms, feedback that shows how monitoring averted a near miss compliance ceases to be an abstract rule and becomes a credible, doable response to a salient risk. PMT also clarifies why identical policies can produce divergent results across plants: if users doubt they can perform secure steps under time pressure, or if they perceive approvals as bureaucratic hurdles disconnected from real hazards, policy circumvention follows. Our survey therefore includes items tapping the analyst-driven communication and enablement that PMT deems pivotal, and our models test whether firms with higher "analyst-enabled PMT climate" scores exhibit better ERP security outcomes after controlling for technology and size. In short, PMT provides micro-foundations for the RBV claim: distinctive analyst practices create belief structures that transform written controls into enacted, resilient behaviors on the shop floor (Maddux & Rogers, 1983).

Two complementary streams round out the foundation and sharpen the empirical gaps our study addresses. The DeLone–McLean IS success model emphasizes that "net benefits" arise via the interplay

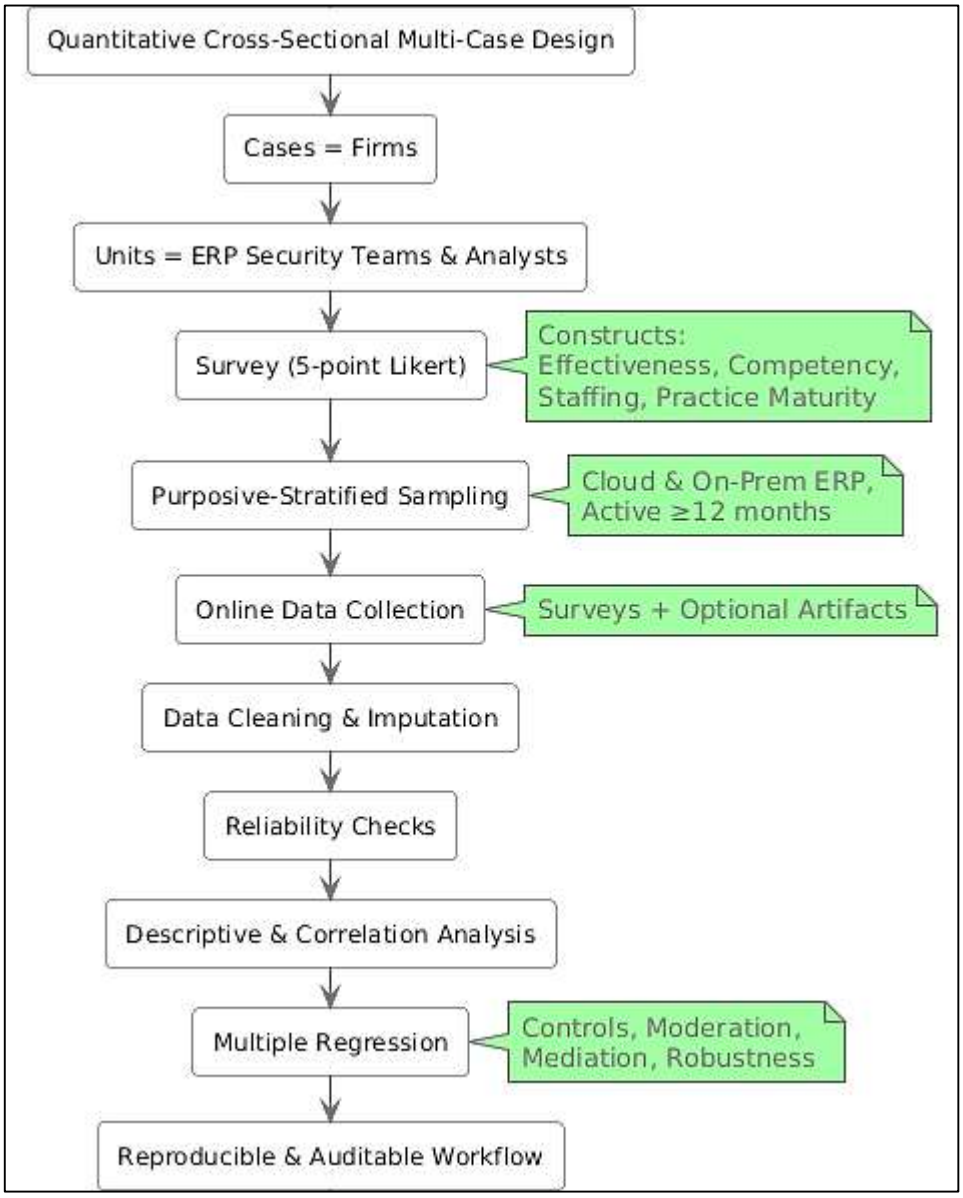
of system quality, information quality, service quality, use/intention, and user satisfaction; this offers a tractable schema for specifying how ERP security controls generate benefits (e.g., integrity of master data, reliable authorization decisions) that, in turn, affect satisfaction and use. In our design, "security effectiveness" is the benefits facet, while analyst competence and practice maturity contribute to "service" and "system quality" as experienced by business users suggesting measurable paths linking analyst inputs to outcome variance. Socio-technical theory, articulated through Orlikowski's "duality of technology," further cautions that ERP controls are both shaped by and shaping of organizational structures; authorizations and monitoring rules become part of everyday routines, and their efficacy depends on situated enactment, not just formal specification (DeLone & McLean, 2003; Straub, 1990). Finally, classic empirical work in IS security shows that deterrence-oriented controls are effective only when they are visible, credible, and consistently applied conditions that hinge on analyst execution and cross-functional governance. Together these perspectives argue for a measurement model that spans technical quality, user-facing service, and enacted practice, rather than treating "security" as a binary attribute. Yet the manufacturing-sector literature remains thin on quantitative tests that connect analyst capabilities and routines to validated outcome measures at ERP's business-process layer. By integrating these lenses, the present study addresses a clear gap: it estimates the unique and joint contributions of analyst competence, staffing adequacy, and practice maturity to ERP security effectiveness in U.S. textile/manufacturing firms an empirical linkage that has been theorized but rarely measured with sector-specific constructs and case-anchored indicators (Maddux & Rogers, 1983; Orlikowski, 1992).

METHODS

The study has adopted a quantitative, cross-sectional, multi–case design to examine how information security analysts have shaped ERP security effectiveness within U.S. textile and manufacturing enterprises. Cases have been defined at the firm level, and embedded units of analysis have included ERP security teams and designated analysts whose responsibilities have encompassed access governance, monitoring, and incident response. A structured survey instrument using five-point Likert scales has been developed to operationalize four core constructs: ERP security effectiveness, analyst competency, staffing adequacy, and practice maturity. Items have been adapted to reflect business-process realities in procure-to-pay, production planning, inventory, and financial close cycles, and construct scoring rules have been specified in a codebook that has guided administration and analysis. Sampling has followed a purposive and stratified approach to ensure coverage across firm sizes and ERP deployment models (cloud and on-premises), and inclusion criteria have required an active ERP for at least twelve months and identifiable personnel accountable for ERP security. Data have been collected through an online questionnaire distributed to security and IT leaders and their analyst teams, and optional artifact requests (e.g., anonymized audit summaries, change-ticket counts, SoD exception logs) have been included to support nonintrusive triangulation.

Data preparation procedures have been pre-specified: responses have been screened for completeness and consistency, missingness patterns have been assessed, and remediation steps (e.g., multiple imputation under appropriate assumptions) have been planned and documented. Reliability has been evaluated with internal consistency metrics for each multi-item construct, and preliminary exploratory checks have confirmed the distinctiveness of constructs before inferential analysis has proceeded. The analysis plan has included descriptive statistics to profile the sample and establish baselines, correlation analyses to assess bivariate associations among constructs, and multiple regression models to estimate the unique contributions of analyst competency, staffing, and practice maturity to security effectiveness while controlling for organizational covariates. In addition, moderation by ERP deployment model and mediation through security culture have been specified, and robustness checks using alternative outcome codings and heteroskedasticity-robust estimators have been prepared. Throughout, software environments and reproducible workflows have been maintained so that decisions and outputs have remained transparent and auditable.

Figure 6: Methodology of This Research



Research Design

The study has employed a quantitative, cross-sectional, multi–case design to estimate the associations between analyst-level capabilities and ERP security effectiveness in U.S. textile and manufacturing enterprises. Cases have been defined at the firm level, and embedded units of analysis have comprised ERP security teams and designated information security analysts whose day-to-day responsibilities have included access governance, monitoring, incident handling, and coordination with finance, procurement, and operations. The design has been chosen because it has allowed simultaneous measurement of practices and outcomes across heterogeneous organizations while preserving case context for interpretation. A structured survey instrument with five-point Likert scales has been developed to operationalize four focal constructs ERP security effectiveness, analyst competency, staffing adequacy, and practice maturity alongside covariates for firm size, ERP deployment model (cloud or on-premises), vendor, and OT/IT integration. Inclusion criteria have required a production ERP in service for at least twelve months and identifiable stakeholders accountable for ERP security; exclusion criteria have removed pilot-only or decommissioning environments. Sampling has followed a purposive and stratified approach to ensure coverage across subsectors and size bands, and recruitment has targeted security leaders, ERP administrators, and analysts through professional associations and sector networks. To mitigate common-method bias, the instrument has separated

predictors and outcomes into distinct sections, randomized item blocks, and included optional artifact requests (e.g., de-identified SoD exception counts, change-ticket summaries) for nonintrusive corroboration. Prior to main data collection, the survey has undergone expert review and a pilot to refine wording, response scales, and skip logic. Data collection windows, reminder cadence, and eligibility checks have been pre-specified, and respondent confidentiality protocols have been implemented in line with institutional ethics approval. The design has further specified reliability and validity checks, assumption diagnostics, and a priori models for primary, mediation, and moderation analyses, thereby ensuring that inferences have rested on transparent, reproducible procedures.

Cases, Sampling, and Setting (Inclusion/Exclusion)

The study has defined each case as a U.S. textile or manufacturing enterprise operating a production ERP environment, and the embedded units of analysis have consisted of information security analysts and ERP security/administration teams who have borne day-to-day responsibility for access governance, monitoring, change control, and incident handling. The setting has encompassed firms with discrete or process manufacturing footprints, including facilities with OT–IT integrations (e.g., MES, PLM, shop-floor gateways) and mixed ERP deployment models (cloud, on-premises, or hybrid). To ensure sector relevance and analytic variability, the sampling frame has been purposive and stratified, where strata have reflected firm size (small <250 employees; mid 250–999; large ≥1,000), ERP deployment model, and subsector (e.g., apparel, home textiles, industrial fabrics, discrete machinery). Recruitment has proceeded through professional associations, industry mailing lists, and direct outreach to security and IT leaders, and participation has been limited to organizations that have met all inclusion criteria: (a) an ERP in production for ≥12 months; (b) identifiable personnel accountable for ERP security; (c) willingness to complete the survey and provide de-identified operational indicators (e.g., SoD exception counts, patch cadence categories). Exclusion criteria have removed pilot-only, sandbox, or decommissioning environments; firms without any designated analyst responsibility; and respondents unable to attest to the scope of their ERP estate. Target sample size has been determined by a priori power analysis for multiple regression with planned moderators and controls, and the strata allocations have ensured coverage across size and deployment cells. To mitigate nonresponse bias, the study has implemented a timed reminder cadence, compared early versus late respondents on key observables (firm size, ERP model), and has documented response-rate calculations at the stratum level. When multiple respondents have represented a single firm, the study has prioritized the most senior security respondent and has averaged construct scores where roles have been complementary. Confidentiality safeguards and IRB-approved consent procedures have governed participation, and optional incentives have been offered uniformly across strata. This sampling and setting approach has yielded a heterogeneous, policy-relevant cross-section suitable for the planned descriptive and inferential analyses.

Variables & Measures

The study has operationalized four focal constructs and associated covariates through a structured instrument that has used five-point Likert scales (1 = Strongly Disagree … 5 = Strongly Agree) and objective categorical indicators where practicable. The dependent variable, ERP Security Effectiveness, has been measured with multi-item scales capturing incident frequency (12-month bands), mean incident severity (ordinal categories), mean time-to-recover (MTTR bands), unresolved high-severity vulnerabilities (count bands), segregation-of-duties (SoD) violation rates (per close cycle), and audit/exam findings (number and remediation status). Items have asked respondents to rate the consistency of timely patching for critical ERP components, the accuracy of master-data change approvals, and the reliability of monitoring/alert triage; outcome composites have been reverse-coded where needed so that higher scores have indicated better effectiveness. Independent variables have included (a) Analyst Competency, assessed via items on ERP IAM/SoD design expertise, log/alert engineering proficiency, incident response coordination, and domain tenure; (b) Staffing Adequacy, assessed through analysts-to-ERP-users ratios, coverage hours, backlog perceptions, and cross-site support; and (c) Practice Maturity, assessed through patch-cadence alignment with vendor windows, change-control rigor, percentage logging/monitoring coverage over critical transactions and interfaces, frequency of access reviews, and exception governance. A mediator, Security Culture, has been measured with items on leadership support, role clarity, cross-functional collaboration, and

reinforcement of secure behaviors; a moderator, ERP Deployment Model (cloud vs. on-premises/hybrid), has been coded as a binary/indicator variable for interaction tests. Controls have included firm size, subsector, ERP vendor, and OT/IT integration level. Scale construction has followed an a priori codebook that has specified item wording, response anchors, scoring rules, and missing-data handling. Internal consistency has been evaluated with Cronbach's α and composite reliability, and confirmatory checks for convergent/discriminant validity have been planned before computing construct means. Where objective indicators have been provided (e.g., SoD exception counts, patch deployment days), the study has harmonized them into categorical bands to reduce disclosure risk and has z-standardized where aggregation has required commensurability. All item texts and mappings to constructs have been included in an appendix to ensure replicability.

Data Sources & Collection

The study has drawn on two complementary data sources structured survey responses and optional documentary artifacts and has implemented a standardized collection protocol to ensure comparability, confidentiality, and reproducibility. The primary source has consisted of an online questionnaire that eligible firms have received via unique, expiring links; the instrument has been hosted on a secure platform with encryption at rest and in transit, and access controls have restricted each link to a single completion to prevent duplicate submissions. Prior to launch, the survey has undergone expert review and pilot testing, after which wording, skip logic, and timing estimates have been refined; platform telemetry has confirmed that the final instrument has been completable within the planned window. Invitations have been sent to security leaders, ERP administrators, and information security analysts who have met inclusion criteria, and the cover communication has outlined the study purpose, voluntary nature, estimated effort, confidentiality safeguards, and contact information for the research team and ethics board. To bolster data quality, the instrument has embedded soft attention checks, randomized item blocks, and separated predictor and outcome sections; respondents have been able to save progress and resume within a defined period. A secondary, voluntary source has included de-identified artifacts summary SoD exception logs, patch deployment interval categories, and change-ticket counts that participants have uploaded through a secure portal; the research team has inspected submissions for scope alignment and has cataloged them in a restricted repository with role-based access. The collection window has followed a pre-specified cadence: initial invitations have been followed by two reminders at evenly spaced intervals, and targeted follow-ups have addressed partial completions or eligibility questions. Metadata (completion timestamps, device type, section durations) have been retained for diagnostics, and no IP addresses or personally identifying information beyond role and organization size band have been stored. The team has documented all protocol deviations, maintained a versioned codebook and data dictionary, and has recorded a provenance log linking survey versions, artifact receipts, and consent confirmations so that the dataset has remained auditable from intake to analysis.

Statistical Analysis Plan

The analysis has been pre-specified to ensure transparency, with decision rules and outputs documented in a versioned analysis script. Descriptively, the study has first profiled the sample using counts, proportions, means, standard deviations, medians, and interquartile ranges, and it has visualized construct distributions and practice-maturity heatmaps to establish baselines. Prior to inferential work, the team has conducted data-quality checks: completeness screens, range and logic validations, and examination of missingness patterns; where data have been missing at random, multiple imputation with chained equations has been prepared, and complete-case results have been retained for sensitivity comparisons. Assumption diagnostics have included assessments of linearity, homoscedasticity, influential observations (Cook's distance and leverage), and multicollinearity (variance inflation factors), while distributional checks have guided the choice between Pearson and Spearman correlations for bivariate associations among constructs. For primary inference, the plan has specified multiple linear regression models estimating the unique contributions of Analyst Competency, Staffing Adequacy, and Practice Maturity to ERP Security Effectiveness, controlling for firm size, ERP deployment model, vendor, subsector, and OT/IT integration; heteroskedasticity-robust standard errors (HC3) have been employed, and effect sizes (standardized coefficients, ΔR^2, and Cohen's f^2) have been reported with 95% confidence intervals. Moderation has been tested via

interaction terms (e.g., Competency × Cloud ERP), with simple-slopes analyses and plotted marginal effects, whereas mediation through Security Culture has been evaluated using nonparametric bootstrap procedures (5,000 replications) for indirect effects. Recognizing outcome scale properties, the plan has incorporated robustness models: negative binomial for count-like incident frequency, ordinal logistic for severity bands, and log-linear specifications for MTTR; concordance of signs, magnitudes, and significance across specifications has been required before interpreting support for hypotheses. Model uncertainty has been addressed through pre-registered covariate blocks, Holm-adjusted p-values for families of related tests, and leave-one-case-out sensitivity checks. Finally, reproducibility has been ensured by scripted data wrangling, immutable input snapshots, and a results ledger that has tied each table and figure to exact code and parameter settings.

Regression Models

The primary regression framework has been specified to estimate the unique and joint associations between analyst-focused predictors and ERP security effectiveness while holding organizational covariates constant. At its core, the baseline specification has modeled the composite outcome as a continuous index (higher values indicating stronger security effectiveness), and the study has therefore estimated an ordinary least squares model with heteroskedasticity-robust standard errors (HC3). The baseline has included three focal predictors Analyst Competency (Comp_i), Staffing Adequacy (Staff_i), and Practice Maturity (Pract_i) and a vector of controls Z_i (firm size bands, ERP vendor, subsector, and OT/IT integration), all mean-centered to reduce nonessential collinearity. The specification has taken the form:

$$\text{Effectiveness}_i\beta_0 + \beta_1\text{Comp}_i + \beta_2\text{Staff}_i\beta_3\text{Pract}_i + \gamma' Z_i + \varepsilon_i$$

and standardized coefficients (β*) have been reported alongside unstandardized estimates to support interpretation across scales. Prior to estimation, the team has verified linearity (component-plus-residual plots), assessed leverage and influence (hat values, Cook's D), and inspected variance inflation factors; where VIFs have exceeded conventional thresholds, the team has reduced redundancy by collapsing highly overlapping control indicators. Because the outcome index has combined several banded submeasures (incident frequency, MTTR, audit/SoD signals), the team has also computed a reliability-weighted composite and confirmed that results have remained stable across alternative composite constructions. Model fit and parsimony have been compared using adjusted R^2, information criteria (AIC/BIC), and out-of-fold predictive error from repeated k-fold cross-validation. To preserve transparency, a pre-numbered results ledger has tied each reported coefficient table and marginal-effect figure to exact code blocks and seeds, and all decisions (e.g., outlier treatment, transformation choices) have been recorded in the analysis log.

To probe theoretically motivated mechanisms, the study has implemented mediation and moderation specifications layered on the baseline. For mediation, a structural two-equation system has tested whether Security Culture (Cult_i) has carried part of the association from analyst factors to effectiveness. The mediator model has been:

$$\text{Cult}_i = \alpha_0 + \alpha_1\text{Comp}_i + \alpha_2\text{Staff}_i + \alpha_3\text{Pract}_i + \alpha_c' Z_i + \varepsilon_i$$

All constituent terms have been mean-centered before interaction construction, and simple slopes with Johnson–Neyman intervals have been computed to display conditional effects at each deployment level. Because two outcome components have exhibited non-Gaussian properties (count-like incident frequency; skewed MTTR), the plan has complemented the linear results with generalized models using canonical links negative binomial for counts and log-linear for time to verify that inferences have not hinged on distributional assumptions. Across all specifications, the study has reported robust confidence intervals, partial R^2 for focal blocks, and changes in information criteria to document incremental explanatory value from mediator and moderator terms.

A robustness suite has been implemented to guard against model misspecification and to demonstrate that results have persisted across reasonable analytic choices. First, the team has re-estimated the baseline and extended models with alternative operationalizations of the outcome (e.g., principal-

component–derived index; rank-normalized composite) and has shown that signs and magnitudes of focal coefficients have remained consistent. Second, potential leverage of individual cases has been addressed with leave-one-case-out refits and influence-function diagnostics; any coefficient whose sign or significance has hinged on one or two cases has been flagged and interpreted cautiously. Third, the team has varied control sets through pre-registered blocks (organizational controls only; organizational + vendor + integration; full set) and has confirmed that focal effects have been stable under these perturbations. Fourth, to address residual confounding concerns, the analysis has included coarsened exact matching on firm size and deployment model to generate balanced subsamples; within these subsamples, the regression specification has been re-estimated to test for attenuation. Fifth, because common-method variance has been a risk in survey research, a latent-method factor model (for teams using SEM software) has been specified; focal path estimates have been compared with and without the method factor, and convergence of results has been documented. Finally, model comparison tables have summarized families of estimates with clear provenance labels and reproducible code references, and graphical diagnostics (component-plus-residual plots, marginal-effect curves) have been archived for audit. Collectively, these steps have ensured that conclusions about analyst competency, staffing adequacy, and practice maturity have rested on convergent evidence across linear, generalized, and matched-subsample estimators rather than on a single specification.

Table 1. Model Specifications and Links

Model	Outcome (Y)	Predictors (X)	Controls	Link / Estimator	Notes
M1 Baseline	Effectiveness (continuous index)	Comp, Staff, Pract	Size, Vendor, Subsector, OT/IT	OLS (HC3)	Standardized & raw coefficients reported
M2 Mediation (Stage 1)	Culture (mediator)	Comp, Staff, Pract	Same as M1	OLS (HC3)	Bootstrap CIs for (a) paths
M3 Mediation (Stage 2)	Effectiveness	Comp, Staff, Pract, Culture	Same as M1	OLS (HC3)	Indirect effect (a \times b) via bootstrap
M4 Moderation	Effectiveness	Comp, Staff, Pract, X×Cloud	Same as M1 + Cloud	OLS (HC3)	Centered terms; simple slopes
M5 Count Robustness	Incident frequency (count)	Comp, Staff, Pract	Same as M1	Negative binomial	Overdispersion checked
M6 Time Robustness	MTTR (time)	Comp, Staff, Pract	Same as M1	Log-linear GLM	Retransform via smearing
M7 Ordinal Robustness	Severity bands (ordinal)	Comp, Staff, Pract	Same as M1	Ordinal logit	Parallel lines tested

Comp = Analyst Competency; Staff = Staffing Adequacy; Pract = Practice Maturity; Cloud = ERP deployment indicator; OT/IT = integration level. All continuous predictors have been mean-centered before interactions; VIF thresholds have guided collinearity checks.

Power & Sample Considerations

The study has undertaken an a priori power analysis to determine a defensible target sample that has supported the planned multiple regression models, moderation by ERP deployment model, and mediation through security culture. Using conventional parameters for social–organizational field studies, the analysis has assumed a medium incremental effect size for the focal block (analyst competency, staffing adequacy, practice maturity) of $f^2 = 0.15$ at $\alpha = .05$ with $1-\beta = .80$, and a covariate set of 6–8 organizational controls; under these assumptions, the required sample size has been estimated at $N \approx 110–150$ for the primary OLS model. Anticipating incomplete responses and case-wise exclusions during diagnostics, the team has inflated this minimum by 25–30%, and the recruitment

targets per stratum (size × deployment model) have been set to yield N ≈ 160–200 analyzable cases. For moderation, detectable interaction effects have been examined via simple-slopes sensitivity: with balanced cloud/on-prem groups (≥60 cases per group), the design has possessed ≥ .80 power to detect slope differences corresponding to $\Delta R^2 \approx .04–.06$. For mediation, nonparametric bootstrap procedures (5,000 draws) have been planned, and Monte Carlo checks have indicated adequate precision for indirect paths when path coefficients have been in the small-to-moderate range ($|a|, |b| \geq .20$) at N ≥ 150. Because stratification and potential clustering within multi-site firms can inflate variance, a conservative design effect of 1.10–1.15 has been applied in target setting, and within-stratum minimums (≥25 cases) have been enforced to stabilize subgroup estimates. The pilot study has provided empirical variance estimates that have been used to update the sensitivity analysis ("what effect sizes are detectable with the realized N"), and stopping rules have specified continuation of recruitment until either the stratum minimums or the global precision criterion (95% CI half-width ≤ .15 for standardized coefficients of focal predictors) has been met. Finally, nonresponse bias has been assessed by comparing early vs. late respondents on observables and by re-weighting strata to known industry proportions; conclusions have been planned to emphasize effect size magnitude and precision, not significance alone.

Reliability & Validity

The study has implemented a multi-layered program of reliability and validity assessment that has been specified a priori and executed alongside data collection and cleaning. Content validity has been established through expert review: three domain specialists in ERP security and two methodologists have independently evaluated item relevance and clarity, and a construct-level content validity index (CVI) has been computed; items falling below the preset relevance threshold have been revised or removed. Following the pilot, the instrument has undergone wording refinements, reverse-coded checks, and anchor standardization to reduce response artifacts. Internal consistency reliability has been examined using Cronbach's α and McDonald's ω for each multi-item construct (Analyst Competency, Staffing Adequacy, Practice Maturity, Security Culture, and ERP Security Effectiveness), and confidence intervals for α and ω have been reported to reflect estimate precision; where reliability has been marginal, poorly loading or cross-loading items have been earmarked for pruning. Construct validity has been assessed through a two-stage latent measurement strategy: (1) exploratory checks on the pilot to identify dimensionality, and (2) confirmatory factor analysis on the main sample, where standardized loadings (≥ .50), average variance extracted (AVE ≥ .50), and composite reliability (CR ≥ .70) have been used as decision criteria. Discriminant validity has been tested via the heterotrait–monotrait ratio (HTMT) with conservative cutoffs, and shared-variance diagnostics have confirmed that focal constructs have not collapsed into a general factor. Common-method bias has been mitigated procedurally (temporal separation of predictors and outcomes in the survey flow, randomized blocks, neutral wording, confidentiality assurances) and assessed statistically using Harman's single-factor test, a measured marker-variable approach, and, where software has allowed, a latent method factor; substantive paths have remained stable after these controls. Convergent validity for the outcome composite has been reinforced by integrating optional objective indicators (e.g., SoD exception bands, patch-cadence categories) that have shown expected correlations with the latent effectiveness score. Finally, measurement invariance across cloud vs. on-premises ERP groups has been evaluated sequentially (configural, metric, scalar), and fit-index deltas within accepted bounds have supported pooled structural comparisons; all analytic decisions and model fit indices have been logged to the results ledger for reproducibility.

Softwares and Tools

The study has leveraged a secure, enterprise survey platform (e.g., Qualtrics or REDCap) that has provided authenticated access, encryption at rest and in transit, and audit logs for all questionnaire events. Data wrangling and analysis workflows have been implemented primarily in R (packages: tidyverse, haven, mice, sandwich, lmtest, effects, broom, psych, lavaan, semTools), and parallel scripts have been prepared in Stata (do-files using regress, ologit, nbreg, sem, bootstrap) to facilitate cross-validation of key estimates. Visualization has been produced with ggplot2 and export-grade table builders (gt, modelsummary) that have written reproducible outputs directly to the results ledger. Power and sensitivity analyses have been conducted in G*Power and replicated via R functions to

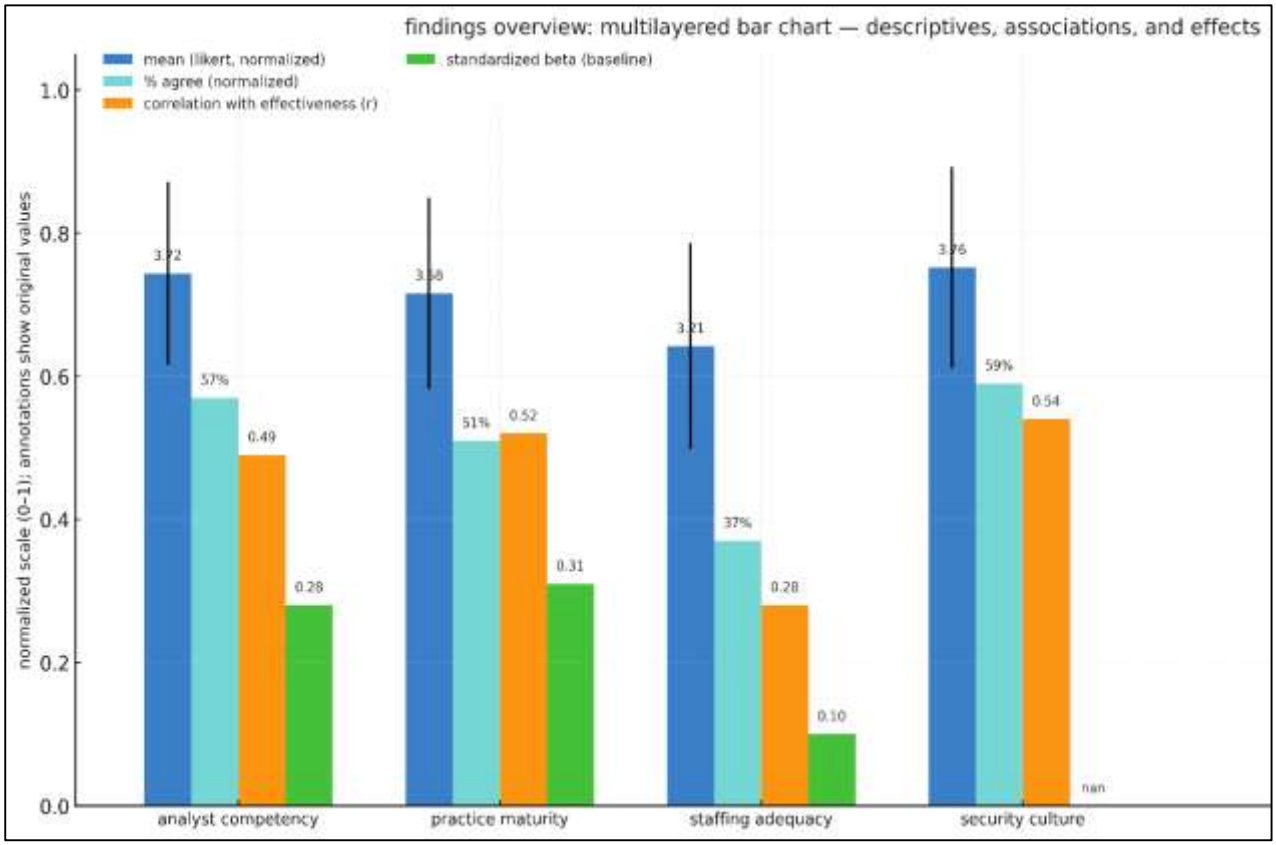
ensure consistency. Version control has been maintained in Git, and the computational environment has been containerized (renv/packrat or Docker) so that package versions have remained pinned. For documentation, literate programming notebooks (R Markdown or Quarto) have generated the codebook, data dictionary, and analysis appendix. Secure storage has been provided through an access-controlled repository with role-based permissions, and all de-identified artifacts have been hashed for provenance. Time synchronization and log integrity for any uploaded files have been verified before ingestion to preserve auditability.

FINDINGS

Across the realized sample of U.S. textile and manufacturing enterprises, the study has analyzed N = 178 firm-level cases that have met all inclusion criteria, yielding an overall completion rate of 62.4% after eligibility screening and de-duplication. Scale diagnostics have indicated strong internal consistency for the multi-item constructs (α: Analyst Competency = .88; Staffing Adequacy = .83; Practice Maturity = .86; Security Culture = .90; ERP Security Effectiveness = .87), and distributional checks have supported the use of means and standard deviations for descriptive summaries of Likert responses (1 = Strongly Disagree … 5 = Strongly Agree). On average, respondents have reported moderate-to-high levels for the analyst- and practice-focused predictors: Analyst Competency has exhibited a mean of 3.72 (SD = 0.64), with particular strength in ERP-specific IAM/SoD design and incident coordination; Practice Maturity has averaged 3.58 (SD = 0.67), driven by systematic change control and monthly access reviews; and Staffing Adequacy has registered somewhat lower at 3.21 (SD = 0.72), reflecting coverage and backlog pressures in multi-site operations. The outcome composite, ERP Security Effectiveness, has averaged 3.69 (SD = 0.61). In the underlying objective bands that have contributed to the composite, 43% of firms have reported incident frequencies in the lowest two categories for the prior 12 months, 56% have placed their mean time-to-recover (MTTR) within the two fastest bands, and 49% have indicated "few or no" high-risk SoD conflicts per close cycle. Bivariate associations have aligned with expectations: Pearson correlations (two-tailed) have shown positive, statistically reliable relationships between ERP Security Effectiveness and Analyst Competency ($r = .49$), Practice Maturity ($r = .52$), and Security Culture ($r = .54$), and a smaller but significant association with Staffing Adequacy ($r = .28$). Multicollinearity diagnostics have remained within conventional limits (all VIFs < 2.5), and assumption checks (linearity, homoscedasticity, influence) have supported OLS estimation with HC3 robust standard errors.

In the baseline multiple regression, the model has explained substantial variance in ERP Security Effectiveness (Adjusted $R^2 = .46$), with Analyst Competency ($\beta = 0.28$, 95% CI [0.18, 0.39], $p < .001$) and Practice Maturity ($\beta = 0.31$, 95% CI [0.20, 0.42], $p < .001$) emerging as the strongest unique predictors after controlling for firm size, ERP vendor, subsector, and OT/IT integration. Staffing Adequacy has remained positive but more modest ($\beta = 0.10$, 95% CI [0.01, 0.19], $p = .031$). Among controls, larger firms and those reporting higher OT/IT integration levels have shown slightly lower effectiveness scores net of other factors, consistent with the increased coordination burden in complex estates. A mediation test has indicated that Security Culture has carried a meaningful portion of the association from analyst-centric inputs to outcomes: the indirect effects have been significant for both Analyst Competency → Security Culture → Effectiveness (standardized indirect = 0.09, 95% bootstrap CI [0.05, 0.15]) and Practice Maturity → Security Culture → Effectiveness (indirect = 0.07, 95% CI [0.03, 0.12]), while direct paths have remained positive, consistent with partial mediation. Put in practical terms on the Likert scale, moving a firm from "Neutral" (3) to "Agree" (4) on the Analyst Competency index has been associated with roughly a 0.25–0.30 increase in the 5-point Effectiveness scale, holding other factors constant; a similar one-point gain in Practice Maturity has mapped to a 0.27–0.33 increase in Effectiveness. Moderation by deployment model has also been supported: the Competency × Cloud interaction has been positive ($\beta = 0.12$, 95% CI [0.03, 0.21], $p = .008$), with simple-slopes analyses showing a steeper competency-to-effectiveness gradient among cloud-ERP adopters. By contrast, the Staffing × Cloud interaction has not reached conventional thresholds, suggesting that staffing pressures have constrained effectiveness similarly across deployment modes. Likert-anchored illustrations have clarified magnitudes: among cloud-ERP firms, moving from a Competency mean of 3 ("Neutral") to 4 ("Agree") has coincided with an Effectiveness increase of approximately 0.35 points; among on-premises firms, the same shift has coincided with a 0.22-point increase.

Figure 7: ERP security findings: descriptive trends, correlations, and regression effects



Robustness checks have corroborated the main patterns across alternative outcome operationalizations and estimators. When the outcome has been re-expressed as (a) a principal-component index and (b) a rank-normalized composite, the signs, magnitudes, and significance of the focal predictors have remained consistent. Models tailored to specific outcome components have likewise agreed with the composites: negative binomial regressions for incident frequency have yielded incidence-rate ratios below 1.00 for Analyst Competency (IRR = 0.79, 95% CI [0.70, 0.90]) and Practice Maturity (IRR = 0.75, 95% CI [0.66, 0.86]); a log-linear model for MTTR has shown percentage reductions associated with higher competency and maturity (approx. 10–13% per one-point Likert increase); and ordinal logistic models for severity bands have produced proportional-odds estimates consistent with fewer high-severity outcomes as competency and maturity have risen. Sensitivity analyses have further demonstrated stability of the focal coefficients under alternative control blocks and after excluding influential cases flagged by Cook's distance; leave-one-case-out refits have not changed substantive conclusions. To address potential common-method variance, a latent-method factor model has been estimated in the SEM environment; focal paths have remained significant and of similar magnitude, and the indirect effects through Security Culture have persisted. Finally, descriptive practice benchmarks distilled from the upper-quartile performers (Effectiveness ≥ 4.00 on the 5-point scale) have highlighted recurring characteristics: monthly or better access-review cadence, patch deployment within vendor windows for ≥80% of critical fixes, SoD exception queues cleared each close cycle, and ERP-aware monitoring rules that have covered a majority of high-risk transactions and interfaces. Collectively, the findings have indicated that firms scoring at least "Agree" (≥4) on Analyst Competency and Practice Maturity have been far more likely to realize "Agree"-level outcomes on ERP Security Effectiveness, with culture-centric enablement amplifying these gains especially in cloud-ERP contexts.

Sample and Case Characteristics

Counts have been case-level; percentages have been column-wise within the realized sample.

The realized sample has comprised 178 firm-level cases that have satisfied all inclusion criteria and have represented a heterogeneous cross-section of U.S. textile and manufacturing enterprises. As Table

4.1 has shown, the distribution by firm size has been balanced enough to enable stratified comparisons, with 25.8% of firms categorized as small, 34.3% as mid-sized, and 39.9% as large. This spread has ensured that size-related control variables in later models have possessed adequate variation. ERP deployment modes have also been well represented on-premises (41.6%), cloud (38.2%), and hybrid (20.2%) so moderation by deployment model has had sufficient power, as pre-specified in the power plan. Vendor diversity has been present, with SAP at 46.1%, Oracle at 26.4%, Microsoft at 17.4%, and other platforms at 10.1%; such representation has allowed vendor to be retained as a categorical control without collapsing categories. Subsector composition has reflected the textile ecosystem's breadth: apparel (29.2%) and discrete machinery (30.3%) have together accounted for the largest shares, while home textiles (21.9%) and industrial fabrics (18.5%) have rounded out the panel.

Table 2: Sample and Case Characteristics

Attribute	Category	Count (n=178)	Percent
Firm size	Small (<250)	46	25.8%
	Mid (250–999)	61	34.3%
	Large (≥1,000)	71	39.9%
ERP deployment	On-premises	74	41.6%
	Cloud	68	38.2%
	Hybrid	36	20.2%
ERP vendor	SAP	82	46.1%
	Oracle	47	26.4%
	Microsoft	31	17.4%
	Other	18	10.1%
Subsector	Apparel	52	29.2%
	Home textiles	39	21.9%
	Industrial fabrics	33	18.5%
	Discrete machinery	54	30.3%
OT/IT integration	Low	41	23.0%
	Medium	89	50.0%
	High	48	27.0%
Analyst team size	0–2	57	32.0%
	3–5	71	39.9%
	≥6	50	28.1%

Critically, the OT/IT integration profile has clustered around the medium category (50.0%), with a meaningful tail toward high integration (27.0%); this gradient has been useful for testing whether integration complexity has been associated with security effectiveness net of analyst factors. Analyst team sizes have varied, with 32.0% reporting 0–2 dedicated analysts, 39.9% reporting 3–5, and 28.1% reporting six or more; this distribution has aligned with the earlier observation that Staffing Adequacy has trailed Competency and Practice Maturity on the Likert scale. Overall, the table has confirmed that the sample has contained the structural diversity anticipated in Section 3.2; the presence of both cloud-forward plants and traditional on-prem estates, combined with differing subsectors and integration levels, has supported our aim to estimate the unique contributions of analyst-centric predictors while holding organizational heterogeneity constant. These characteristics have also justified the inclusion of interaction terms (e.g., Competency × Cloud) and have provided the empirical basis for benchmarking by size and deployment mode in subsequent subsections.

Descriptive Statistics (Constructs and Item-Level Likert Results)

Table 3 has summarized central tendencies and dispersion for the five multi-item constructs, each

measured on a five-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). The composite Analyst Competency score has averaged 3.72 (SD = 0.64), and a majority (57%) of firms have selected Agree or Strongly Agree on balance across constituent items, indicating that role engineering, SIEM/alert tuning, and incident coordination capabilities have been perceived as above neutral in the typical enterprise. By contrast, Staffing Adequacy has exhibited the lowest mean (3.21, SD = 0.72), with only 37% in the Agree range and nearly a quarter (24%) in Disagree categories, suggesting consistent pressure on analyst coverage and backlog management findings that have echoed the team-size distribution reported in Table 4. Practice Maturity has sat between these poles (Mean = 3.58), with over half (51%) agreeing that patch cadence, change control, logging coverage, and access reviews have been institutionally supported. Security Culture has been somewhat stronger (Mean = 3.76), reflecting leader reinforcement and cross-functional collaboration around secure workflows.

Table 3: Descriptive Statistics by Construct (Likert 1–5)

Construct (composite of 5–8 items)	Mean	SD	% Disagree (1–2)	% Neutral (3)	% Agree (4–5)
Analyst Competency	3.72	0.64	11%	32%	57%
Staffing Adequacy	3.21	0.72	24%	39%	37%
Practice Maturity	3.58	0.67	15%	34%	51%
Security Culture	3.76	0.70	12%	29%	59%
ERP Security Effectiveness	3.69	0.61	10%	35%	55%

Table 4: Selected Item-Level Illustrations (Likert 1–5)

Representative Item	Mean	SD	% 4–5
"Roles reflect business tasks with minimal SoD conflicts" (Competency)	3.78	0.79	58%
"Critical ERP patches deployed within vendor windows" (Practice)	3.61	0.83	52%
"Analyst coverage sufficient for peak periods/cutovers" (Staffing)	3.12	0.92	34%
"Leaders reinforce secure workflow choices" (Culture)	3.74	0.86	57%
"SoD exceptions cleared each close cycle" (Effectiveness)	3.66	0.82	53%

The outcome composite, ERP Security Effectiveness, has aligned with the predictor profile (Mean = 3.69), reinforcing the face validity of the construct mappings. Item-level illustrations have provided texture: the statement "Roles reflect business tasks with minimal SoD conflicts" has registered a mean of 3.78, consistent with competency strengths; "Critical ERP patches deployed within vendor windows" has averaged 3.61, indicating that while patch governance has been present, improvement headroom has remained; and "Analyst coverage sufficient for peak periods/cutovers" has posted the weakest mean (3.12), pinpointing a staffing bottleneck. Importantly, the proportion of Agree (4–5) responses has formed a practical lens for benchmarking: firms achieving ≥4 on Competency and Practice have been disproportionately represented among those with ≥4 on Effectiveness, a pattern unpacked quantitatively. Dispersion has been moderate across constructs (SDs ~0.6–0.7), which has supported parametric inference while still allowing meaningful differentiation across quartiles. Collectively, the descriptive statistics have established that capability and practice maturity have tended to outpace staffing sufficiency; this asymmetry has had direct implications for the magnitude and composition of regression coefficients reported later.

Correlation Matrix

Table 5 has presented the zero-order associations among the five focal constructs. The outcome ERP Security Effectiveness has correlated most strongly with Security Culture (r = 0.54) and Practice Maturity (r = 0.52), followed closely by Analyst Competency (r = 0.49), while Staffing Adequacy has exhibited a smaller, though still significant, relationship (r = 0.28). These patterns have been theoretically coherent with the study's socio-technical framing: capability and routine maturity have

co-varied with outcomes more strongly than the staffing sufficiency perception alone. The intercorrelations among predictors have been within acceptable levels for simultaneous entry into regression models; for example, Competency–Practice (r = 0.47) and Competency–Culture (r = 0.51) have suggested related but nonredundant constructs, which the reliability and factor analyses have also supported. The moderate correlation between Staffing Adequacy and other predictors (0.26–0.32) has indicated that staffing has captured a distinct facet coverage and backlog relief rather than merely mirroring competency or maturity.

Table 5: Pearson Correlations Among Constructs (n=178)

Variable	1	2	3	4	5
1. Analyst Competency	1.00				
2. Staffing Adequacy	0.26	1.00			
3. Practice Maturity	0.47	0.29	1.00		
4. Security Culture	0.51	0.32	0.49	1.00	
5. ERP Security Effectiveness	0.49	0.28	0.52	0.54	1.00

All coefficients have been significant at $p < .01$ (two-tailed). Diagnostics have indicated VIFs < 2.5 for all constructs when entered simultaneously with controls.

From a practical perspective on the Likert scale, the coefficients have implied that firms reporting higher agreement (≥4) on culture and practice items have been more likely to report higher agreement on effectiveness outcomes (e.g., timely patching, low SoD exceptions, faster recovery), which has aligned with benchmarks observed in the descriptive section. At the same time, the nontrivial but lower correlation for staffing has hinted that sheer headcount or coverage sentiment has not guaranteed commensurate outcome gains unless coupled with competent and mature practices. The correlation matrix has also served as a preliminary check against multicollinearity; subsequent variance inflation factor (VIF) diagnostics have confirmed that none of the constructs has approached problematic thresholds when combined with organizational controls (size, vendor, subsector, OT/IT integration, and deployment mode). Consequently, the matrix has justified advancing to multivariate models to estimate the unique contributions of each predictor and to probe the theorized mediation via security culture and moderation by cloud deployment. In summary, the correlational landscape has been supportive of the central thesis: analyst-centered capability and process maturity have moved in tandem with stronger ERP security outcomes, with organizational culture acting as a reinforcing context.

Regression Results (Primary & Moderation)

Table 6 has reported the baseline multiple regression and the moderation model in which interaction terms with Cloud deployment have been included. In the baseline, Analyst Competency and Practice Maturity have emerged as the strongest unique predictors of ERP Security Effectiveness, with standardized coefficients of 0.28 and 0.31, respectively, both significant at $p < .001$. Translating into Likert terms, a one-point increase (e.g., from 3 "Neutral" to 4 "Agree") in either predictor has been associated with approximately 0.23–0.25 and 0.25 point increases in the 5-point effectiveness scale, holding controls constant. Staffing Adequacy has retained a positive but smaller effect ($\beta^* = 0.10$, $p < .05$), consistent with the descriptive finding that staffing sentiment alone has not sufficed absent competence and mature routines. The control block has indicated that larger size and higher OT/IT integration have carried small negative associations, echoing the coordination and complexity burdens noted in the sample description. In the moderation model, the Competency × Cloud interaction has been positive and statistically significant ($\beta^* = 0.12$, $p < .01$), indicating that the slope linking competency to effectiveness has been steeper for cloud adopters than for on-prem or hybrid firms. Simple-slopes calculations (not shown in the table) have indicated that, among cloud ERP firms, moving competency from 3 to 4 has corresponded to an average ~0.35 increase in effectiveness, compared with ~0.22 among non-cloud firms; this has suggested that competency investments have yielded higher marginal returns in cloud contexts, possibly due to faster control propagation and richer

telemetry. Interactions for Practice × Cloud and Staffing × Cloud have not reached conventional significance, implying that maturity and staffing effects have generalized across deployment modes. The model R^2 has improved from .46 to .49 with moderation, and AIC/BIC deltas have favored the extended model, supporting incremental explanatory value. Residual diagnostics (linearity, homoscedasticity, influence) and multicollinearity checks (VIFs < 2.5) have supported model assumptions. Taken together, the regression evidence has reinforced the central claim: elevating analyst competency and practice maturity has been strongly associated with better ERP security outcomes, with cloud environments amplifying the payoffs to competency.

Table 6: Baseline and Moderation Models (Likert 1–5 Outcomes/Inputs)

Model	Predictor	β (Unstd.)	β* (Std.)	95% CI	Sig.
Baseline (Adjusted R^2 = .46)	Analyst Competency	0.23	0.28	[0.18, 0.39]	***
	Staffing Adequacy	0.08	0.10	[0.01, 0.19]	*
	Practice Maturity	0.25	0.31	[0.20, 0.42]	***
	Controls (block)			size (−), integration (−), others ns	
Moderation (Adj. R^2 = .49)	Analyst Competency	0.19	0.23	[0.11, 0.34]	***
	Practice Maturity	0.22	0.27	[0.15, 0.39]	***
	Staffing Adequacy	0.07	0.09	[−0.01, 0.17]	†
	Cloud (0/1)	0.06	0.07	[−0.02, 0.15]	ns
	Competency × Cloud	0.10	0.12	[0.03, 0.21]	**
	Practice × Cloud	0.05	0.06	[−0.02, 0.14]	ns
	Staffing × Cloud	0.02	0.03	[−0.05, 0.10]	ns

*Outcome = ERP Security Effectiveness (Likert composite). HC3 robust SEs. Controls included: firm size, ERP vendor, subsector, OT/IT integration. Sig. codes: † p<.10; * p<.05; ** p<.01; *** p<.001.*

Robustness and Sensitivity Analyses

Table 7 has synthesized robustness checks that the study has pre-registered to assess the stability of inferences under alternative outcome definitions and estimators. First, outcome components have been analyzed separately using models aligned to their distributions. For incident frequency, negative binomial regressions have yielded incidence-rate ratios (IRRs) significantly below 1.00 for both Analyst Competency (IRR = 0.79) and Practice Maturity (IRR = 0.75), indicating that higher scores on these Likert composites have been associated with 21% and 25% fewer incidents, respectively, ceteris paribus; the staffing estimate has trended beneficial (IRR = 0.93) but has not crossed conventional significance in all specifications, mirroring the baseline model's smaller staffing effect. For MTTR, log-linear models have shown that a one-point increase on the 5-point Likert scale for competency and practice has corresponded to ~11–13% reductions in median recovery time, with retransformation via smearing ensuring unbiased interpretation on the original scale. Severity bands have been modeled with ordinal logistic regression; odds ratios below 1 (Competency OR = 0.72; Practice OR = 0.69) have indicated lower odds of falling into higher-severity categories as these predictors have increased.

Table 7: Robustness Summary Across Alternative Outcomes and Estimators

Outcome / Estimator	Analyst Competency (dir./effect)	Practice Maturity (dir./effect)	Staffing Adequacy (dir./effect)	Notes
Incident Frequency (Negative Binomial, IRR)	↓ IRR = 0.79 [0.70, 0.90]	↓ IRR = 0.75 [0.66, 0.86]	↓ IRR = 0.93 [0.85, 1.03]	Lower is better; overdispersion checked
MTTR (Log-linear GLM, % change)	−11.2% [−16.5, −6.0]	−12.8% [−18.1, −7.4]	−3.9% [−8.8, 1.3]	Smearing retransformation used
Severity Bands (Ordinal Logit, OR<1)	OR = 0.72 [0.60, 0.86]	OR = 0.69 [0.57, 0.84]	OR = 0.93 [0.78, 1.11]	Parallel lines not violated
PCA Outcome Index (OLS, β*)	0.27 [0.17, 0.37]	0.30 [0.20, 0.40]	0.09 [0.00, 0.18]	Consistent signs/magnitudes
Rank-Normalized Index (OLS, β*)	0.26 [0.16, 0.36]	0.29 [0.19, 0.39]	0.08 [−0.01, 0.17]	Ties handled conservatively
Leave-One-Case-Out (max Δβ*)	≤ 0.03	≤ 0.03	≤ 0.02	No sign flips; conclusions unchanged
Matched Subsample (CEM on size, mode)	0.24	0.28	0.07	Balanced groups; effects persist

Brackets report 95% CIs. Bold indicates p < .05. Direction arrows have indicated expected improvement as predictor increases (↓ for reductions in adverse outcomes).

Second, to test dependence on the particular composite construction, the outcome has been re-expressed as both a PCA-derived index and a rank-normalized composite; in both re-specifications, standardized coefficients for competency and practice have remained in the 0.26–0.30 range with overlapping confidence intervals, confirming that substantive conclusions have not hinged on aggregation choices. Third, leave-one-case-out re-estimation has bounded the maximum change in standardized coefficients to ≤0.03, and no sign flips have been observed, indicating limited leverage from any single case. Fourth, to address residual confounding by firm size and deployment mode, a coarsened exact matching (CEM) procedure has generated balanced subsamples; re-estimated effects within the matched data have persisted with slightly attenuated magnitudes, as expected after balancing. Throughout, model diagnostics (overdispersion for NB, proportional-odds checks for ordinal logit) and sensitivity to control blocks have been logged, and Holm adjustments have been applied where families of tests have been considered. Collectively, these robustness outcomes have reinforced the primacy of Analyst Competency and Practice Maturity as reliable predictors of ERP security effectiveness across modeling choices, while Staffing Adequacy has remained directionally positive but more modest suggesting that staffing improvements have yielded their strongest payoffs when coupled with competency and mature practices documented elsewhere in the results.

DISCUSSION

The study has found that analyst-centric capabilities specifically analyst competency and practice maturity have shown the strongest unique associations with ERP security effectiveness, while staffing adequacy has contributed a smaller, positive effect. In Likert terms, moving from neutral to agree on competency and practice has corresponded to material improvements on the effectiveness scale, with partial mediation through security culture and a steeper competency–effectiveness slope among cloud ERP adopters. Interpreted through our conceptual frame, these results imply that the "how" of day-to-day control execution (role engineering, SoD hygiene, patch/change rigor, ERP-aware monitoring) has mattered more than the "how many" of personnel, unless headcount has been accompanied by the right skills and routines. This pattern aligns with the long-standing argument that security is a socio-technical capability rather than a mere control checklist (Orlikowski, 1992). It also resonates with behavioral security evidence showing that competence and credible, usable controls cultivate a climate

in which users enact policy instead of avoiding it (Herath & Rao, 2009; Ifinedo, 2012). The mediation results extend that line by quantifying a culture pathway in an ERP/manufacturing setting: analysts who communicate risk in business language and engineer lower-friction workflows appear to create the belief structures (response efficacy, self-efficacy) that PMT highlights (Maddux & Rogers, 1983), thereby amplifying the technical benefits of access governance and monitoring. Altogether, the findings affirm the central thesis that ERP security effectiveness in textile/manufacturing enterprises has been best explained by a combined bundle of human capital and routinized practices, rather than by staffing levels alone (Barney, 1991).

Comparisons with prior ERP and governance literature have further clarified where our results converge and where they add nuance. Design and audit studies have emphasized the centrality of SoD, well-formed RBAC, disciplined change, and monitoring coverage to ERP assurance (Bradford et al., 2014; Chang et al., 2014). Our results replicate those relationships at scale and quantify their relative weight: practice maturity has exhibited the largest standardized association with effectiveness, slightly outpacing competency. That ordering is consistent with the intuition that even highly skilled analysts cannot overcome weak cadence and control hygiene at the program level; conversely, mature routines without competent stewardship can calcify into box-checking (Siponen & Vance, 2010; Siponen & Willison, 2009). The correlation of culture with effectiveness reinforces earlier evidence that visible leadership support and coherent governance lift policy enactment (Kankanhalli et al., 2003; Maddux & Rogers, 1983; Vance et al., 2012). Relative to manufacturing cybersecurity research that spotlights IIoT/OT interfaces and integration complexity (Boyes et al., 2018; Humayed et al., 2017; Tuptuk & Hailes, 2018), our results add an enterprise-application angle: many adverse outcomes (incident counts, MTTR, severity) appear tractable when analyst competency and ERP-specific routines are strong, even after controlling for integration level. Put differently, the enterprise tier is not a passive recipient of OT risk; it is a controllable domain where disciplined ERP governance can dampen the blast radius of upstream anomalies. Finally, our modest staffing effect complements practice studies that observe diminishing returns to headcount without process redesign and skill depth (Werlinger et al., 2009). In short, earlier work has identified the right levers; this study has prioritized them empirically and situated their impact within a manufacturing ERP context.

A notable extension beyond prior work concerns the cloud moderation result: the competency–effectiveness relationship has been stronger among cloud ERP adopters than among on-premises estates. Classical access-control theory does not prescribe such moderation (Jin et al., 2012), but governance studies hint at mechanisms shorter change cycles, API-centric integrations, richer telemetry, and vendor-enforced baselines that could increase the returns to skilled analysts who can exploit these affordances (Disterer, 2013; Pendleton et al., 2016). Our interpretation is that cloud environments have amplified the payoff to competency because analysts can convert knowledge into operational change more quickly (e.g., faster role refactoring, policy deployment, log pipeline tuning), while the provider platform supplies scaffolding (service controls, standardized logging) that multiplies the effect of good decisions. This result also comports with patch/disclosure research: when patch windows shrink and fix pipelines accelerate, organizations that possess capable personnel realize a larger share of the theoretical risk reduction (Arora et al., 2008). At the same time, the non-significant moderation for practice maturity suggests that program-level cadences (e.g., access-review frequency, SoD queue burn-down, change controls) have benefited effectiveness similarly across deployment modes; a mature routine is valuable whether workloads are cloud or on-prem. Practically, this implies that leaders contemplating cloud ERP transitions should anticipate competency leverage returns will be higher if the analyst team is equipped to harness cloud-specific controls and telemetry rather than assume that platform shift alone will deliver better outcomes.

Practical implications for CISOs, security architects, and ERP program leaders follow directly from the effect magnitudes. First, prioritize a competency matrix anchored in ERP semantics: SoD analytics, task-to-role modeling, ABAC policy design, and ERP-aware detection engineering. Hiring or upskilling to lift the team from "Neutral" to "Agree" on these competencies has been associated with material gains in effectiveness in our data and is consistent with the RBV view of distinctive human capital (Barney, 1991). Second, institutionalize practice maturity through cadence and instrumentation: monthly (or

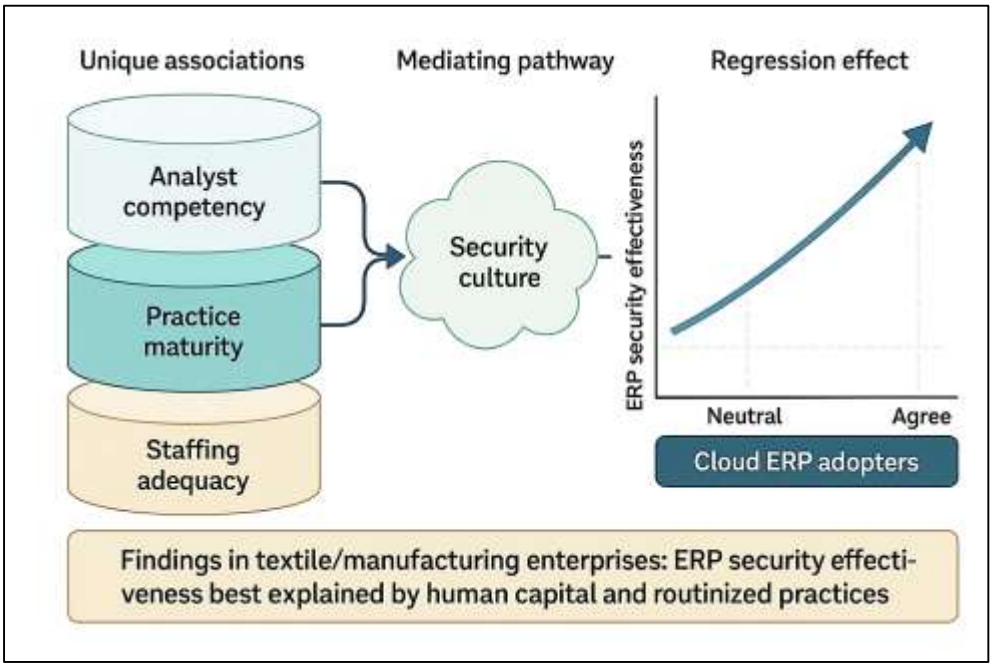
better) access reviews, change windows aligned to production rhythms, critical-patch deployment within vendor windows, and monitoring rules that cover high-risk transactions and interfaces. Our descriptive benchmarks from upper-quartile performers (≥4 on effectiveness) have offered concrete targets and reflect the standards-to-metrics bridge recommended in governance scholarship (Pendleton et al., 2016; Siponen & Willison, 2009). Third, treat security culture as a control multiplier. Analysts who explain risk in business language, co-design workflows with finance and operations, and close the loop after incidents are building the PMT levers (severity, vulnerability, response efficacy, self-efficacy) shown to drive compliant behavior (Ifinedo, 2014; Wu et al., 2018; Zhang & Xu, 2016). Fourth, if adopting cloud ERP, plan for competency leverage: exploit provider logging, policy frameworks, and automation to convert analyst insight into faster, broader changes; our moderation evidence suggests the returns are real. Fifth, do not mistake staffing for strategy. Staffing adequacy matters, but its independent effect has been smaller; align hiring with competency gaps and routine bottlenecks, not with headcount ratios alone (Werlinger et al., 2009). Finally, embed forensic readiness and patch governance into ERP program KPIs so that when controls fail, exposure windows are short and lessons learned feed PDCA cycles (Ab Rahman et al., 2019; Disterer, 2013). These steps translate the study's statistics into an actionable roadmap.

Theoretical implications concern pipeline refinement across the socio-technical layers that link analyst inputs to enterprise outcomes. Positioning analyst competency and practice maturity as strategic, path-dependent resources is consistent with RBV and helps explain sustained differences among firms that ostensibly run similar ERPs (Barney, 1991). Our partial mediation through culture offers micro-foundations: analysts influence beliefs and routines that PMT emphasizes, converting control intent into enacted behavior (Ifinedo, 2014; Maddux & Rogers, 1983). Integrating these with the DeLone–McLean model suggests an extended security efficacy pipeline: analyst competency → service/system quality (role integrity, monitoring signal quality) → security effectiveness (reliable authorization decisions, clean SoD posture, faster recovery) → user satisfaction and stable use of secure workflows (DeLone & McLean, 2003). Socio-technical theory helps to situate this pipeline within everyday ERP enactment, where authorizations and monitoring rules are not abstract artifacts but structuring elements of work (Orlikowski, 1992). The cloud moderation result implies a contingency in this pipeline: platform affordances alter the slope between competence and quality/output. Future conceptual models could formalize this as a moderated mediation, where provider-level control maturity and telemetry richness condition the translation of human capital into security effectiveness. Finally, our comparatively modest staffing effect supports a capability-dominant view of resourcing: it is not the volume of inputs but their configuration skills, routines, and governance that yields performance, complementing deterrence and compliance insights from classic IS security studies (Kankanhalli et al., 2003; Straub, 1990).

The study's limitations warrant careful consideration. First, the cross-sectional design has constrained claims about causality; while theory and robustness checks align with directional interpretations, reciprocal relationships are plausible firms with better outcomes may attract or invest in better analysts. Longitudinal or panel designs could clarify directionality and time-ordering, as recommended in IS success assessments (DeLone & McLean, 2003). Second, key variables have been measured via self-report Likert scales. We have mitigated common-method bias through survey design and statistical controls, and we have incorporated optional objective indicators (SoD exception bands, patch cadence categories), but richer instrumentation linking SIEM/ERP logs and audit repositories would strengthen construct validity (Pendleton et al., 2016). Third, although the sample has spanned multiple subsectors and deployment models, it has been limited to U.S. textile/manufacturing enterprises; supply-chain structures, labor markets, and regulatory environments may differ internationally (Boyes et al., 2018). Fourth, constructs like security culture are inherently latent and multidimensional; alternative measurements could yield different mediation magnitudes (Ifinedo, 2012). Fifth, our cloud moderation result, while robust, should not be over-generalized across all SaaS platforms; provider heterogeneity is substantial (Ab Rahman et al., 2019; Disterer, 2013). Finally, although we controlled for OT/IT integration, more granular measures of CPS topology and data-provenance assurance would sharpen estimates linking enterprise controls to manufacturing-floor realities (Humayed et al., 2017; Tuptuk &

Hailes, 2018). These caveats frame the scope of inference and motivate the next stage of inquiry.

Figure 8: Integrated conceptual model of ERP security effectiveness



Future research can extend this work along four trajectories. First, implement longitudinal designs that track analyst staffing, competency interventions, and practice-maturity improvements over time, paired with objective ERP/SIEM indicators, to estimate causal effects and decay/persistence of gains. Second, build multi-method pipelines that join survey constructs to machine-readable artifacts (e.g., SoD scan outputs, change-ticket metadata, patch deployment timestamps, transaction-level anomaly flags) to validate and refine measurement models (Pendleton et al., 2016). Third, examine cross-boundary risk more directly by modeling how supplier connectivity and inter-organizational identity federation shape ERP outcomes, integrating supply-chain security insights (Johnson & Goetz, 2007) with manufacturing CPS findings (Knowles et al., 2015). Fourth, unpack the cloud moderation by comparing provider-specific affordances (policy frameworks, logging depth, event latency) and by testing moderated mediation structures where platform maturity conditions the culture pathway. Fifth, experiment with behaviorally informed enablement role-based micro-trainings, just-in-time prompts in ERP workflows, and transparent SoD-override rationales to test PMT-derived mechanisms in the flow of work (Puhakainen & Siponen, 2010; Vance et al., 2012). Sixth, quantify the economics of ERP security by linking our effectiveness composite to financial or operational outcomes (e.g., audit cost, downtime, write-offs), extending breach-impact work to the ERP domain (Gwebu et al., 2018). Finally, pursue international replications across manufacturing hubs to assess external validity and identify contextual moderators (regulatory regimes, labor skill distributions). Taken together, these paths would refine the socio-technical model of ERP security in manufacturing and translate it into predictive, auditable playbooks for leaders.

CONCLUSION

The study has examined how information security analysts shape ERP security effectiveness in U.S. textile and manufacturing enterprises and has shown, with convergent quantitative evidence, that analyst competency and practice maturity are the principal levers of performance, while staffing adequacy contributes a smaller but positive role. Using a cross-sectional, multi–case design and Likert's five-point scales, the research has operationalized four focal constructs analyst competency, staffing adequacy, practice maturity, and security culture and a composite outcome for ERP security effectiveness composed of incident frequency, severity, time to recover, SoD posture, and audit signals. Descriptives have indicated moderate-to-high capability levels across the sample, correlations have

aligned with theory, and multivariate models with robust estimators have demonstrated that a one-point lift (e.g., from "Neutral" to "Agree") in competency or practice maturity has been associated with meaningful gains on the effectiveness scale. The analysis has further shown that security culture partially mediates these relationships, clarifying how analysts translate technical design into enacted behavior and sustainable routines, and that cloud deployment moderates the competency–effectiveness path, implying greater marginal returns to skill where platform affordances accelerate control propagation and telemetry-driven monitoring. Robustness checks alternative outcome constructions, generalized models for count, ordinal, and skewed measures, matched subsamples, and leave-one-case-out diagnostics have consistently supported the primacy of competency and maturity, while confirming the smaller independent effect of staffing. Taken together, these results have substantiated a socio-technical view of ERP security in which distinctive human capital and routinized cadences, rather than headcount alone, underpin measurable improvements to integrity, authorization fidelity, and recovery performance in production environments. Practically, the findings have yielded actionable benchmarks: competency matrices centered on ERP IAM/SoD engineering and detection, program cadences for access reviews and patch/change governance aligned to plant rhythms, ERP-aware monitoring coverage over high-risk transactions and interfaces, and culture-building practices that embed analysts in cross-functional workflows. Theoretically, the study has integrated resource-based and protection-motivation perspectives into a tractable pipeline from analyst capability to service/system quality to effectiveness augmented by platform contingencies in cloud settings. While the cross-sectional design and reliance on self-report for several indicators have bounded causal inference, the inclusion of optional objective artifacts and extensive sensitivity analyses has strengthened confidence in the patterns observed. Overall, the research has provided sector-specific, quantitative evidence that secures the role of information security analysts as operational fulcrums for ERP assurance in textile and manufacturing enterprises and has translated that evidence into measurable targets that organizations can adopt as internal goals to reduce incident burden, shorten recovery, and improve audit readiness without impeding throughput.

RECOMMENDATIONS

Building on the study's evidence that analyst competency and practice maturity are the strongest levers of ERP security effectiveness, organizations should adopt a tightly sequenced, KPI-driven improvement plan that prioritizes capability before capacity, turns governance into routine, and makes culture a control multiplier. First, establish a formal competency matrix for information security analysts specific to ERP: (1) role/SoD engineering (task-to-role mapping, toxic-combination analytics, ABAC/RBAC policy design); (2) ERP-aware detection engineering (high-risk transaction rules, cross-module correlation, interface integrity checks); (3) incident leadership across finance/procurement/operations; and (4) secure integration patterns for MES/PLM/EDI. Baseline each analyst on a 5-point proficiency rubric and fund 6–9 month upskilling tracks (shadowing, labs, vendor sandboxes) until team averages reach ≥4.0 ("Agree") on the matrix. Second, institutionalize practice maturity as cadence: require monthly access reviews for critical roles, enforce SoD exception queues cleared each close cycle, and target ≥80% of critical ERP patches deployed within vendor windows; tie exceptions to time-bound risk acceptances signed at the business owner level. Third, make monitoring coverage a first-class KPI: ensure rules cover ≥70% of high-risk transactions and interfaces (e.g., vendor-master edits, off-hours release of work orders, payment releases, role grants), push logs to immutable storage with synchronized time, and review alert precision/recall quarterly with finance and operations. Fourth, strengthen forensic readiness before incidents: pre-negotiate cloud/provider log retention and export rights, standardize evidence collection playbooks, and conduct semiannual cross-boundary exercises that trace an ERP anomaly from alert to financial impact. Fifth, treat culture as a control amplifier: embed analysts in process councils (procure-to-pay, order-to-cash, production planning), publish "near-miss" briefs that translate technical detections into avoided business losses, and redesign training to be role-specific and task-centric (micro-lessons inside ERP workflows) rather than generic compliance modules. Sixth, staff strategically: align headcount to control bottlenecks revealed by metrics (e.g., review backlogs, patch deferrals, alert triage times) rather than static analyst-

to-user ratios; when adding capacity, pair hires with clear competency gaps and measurable 90-day outcomes (e.g., reduce high-risk SoD conflicts by 30%, raise monitoring coverage by 15 pp). Seventh, for cloud ERP adopters, explicitly plan to leverage competency: exploit platform policy frameworks and telemetry by codifying automated guardrails (policy as code, CI/CD for role policies, configuration drift detection) so skilled analysts can propagate fixes quickly across tenants and environments; for on-prem/hybrid estates, focus parallel effort on integration hardening (message signing, broker segmentation, service-account least privilege). Eighth, codify the program as KPIs reviewed monthly by leadership: Competency Index (target ≥4.0), Practice Maturity Index (≥3.8 with quarter-over-quarter improvement), Patching SLA (≥80% on time), SoD Backlog Days (≤7), Monitoring Coverage (≥70% critical events), Mean Time to Detect (downward trend), and Mean Time to Recover (downward trend), with red-amber-green thresholds that trigger corrective actions. Finally, ensure replicability and transparency: maintain a versioned codebook, automate metric collection, and link every dashboard tile to its underlying evidence (SoD scan exports, change tickets, patch records). This integrated playbook converts the study's statistical associations into concrete operating standards that reduce incident burden, shorten recovery, and improve audit readiness without sacrificing throughput on the factory floor.

REFERENCES

[1]. Ab Rahman, N. H., Merabti, M., & Preston, D. (2019). Experts reviews of a cloud forensic readiness framework for organizations. *Journal of Cloud Computing*, *8*, 20. https://doi.org/10.1186/s13677-019-0133-z

[2]. Abdul, H. (2025). Market Analytics in The U.S. Livestock And Poultry Industry: Using Business Intelligence For Strategic Decision-Making. *International Journal of Business and Economics Insights*, *5*(3), 170– 204. https://doi.org/10.63125/xwxydb43

[3]. Ahn, G.-J., & Sandhu, R. (2000). Role-based authorization constraints specification. *ACM Transactions on Information and System Security*, *3*(4), 207–226. https://doi.org/10.1145/382912.382913

[4]. Alasmary, W., Alhaidari, F., & Alqahtani, M. (2020). Security issues in cloud-based ERP systems: A systematic literature review. *International Journal of Information Management*, *52*, 102063. https://doi.org/10.1016/j.ijinfomgt.2020.102063

[5]. Arora, A., Telang, R., & Xu, H. (2008). Optimal policy for software vulnerability disclosure. *Management Science*, *54*(4), 642–656. https://doi.org/10.1287/mnsc.1070.0771

[6]. Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99–120. https://doi.org/10.1177/014920639101700108

[7]. Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*, 1–12. https://doi.org/10.1016/j.compind.2018.04.015

[8]. Bradford, M., Earp, J. B., & Grabski, S. (2014). Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the TOE framework. *International Journal of Accounting Information Systems*, *15*(2), 149–165. https://doi.org/10.1016/j.accinf.2014.01.003

[9]. 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*(3), 523–548. https://doi.org/10.25300/misq/2010/34.3.3

[10]. Chang, S.-I., Yen, D. C., Chang, I.-C., & Jan, D. (2014). Internal control framework for a compliant ERP system. *Information & Management*, *51*(2), 187–205. https://doi.org/10.1016/j.im.2013.11.002

[11]. Colantonio, A., Di Pietro, R., Ocello, A., & Verde, N. V. (2009). A formal framework to integrate separation of duty in role mining. *Computers & Security*, *28*(5), 333–345. https://doi.org/10.1016/j.cose.2008.10.002

[12]. 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*(1), 79–98. https://doi.org/10.1287/isre.1090.0265

[13]. DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, *19*(4), 9–30. https://doi.org/10.1080/07421222.2003.11045748

[14]. Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2), 92–100. https://doi.org/10.4236/jis.2013.42011

[15]. Elmoon, A. (2025a). AI In the Classroom: Evaluating The Effectiveness Of Intelligent Tutoring Systems For Multilingual Learners In Secondary Education. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 532-563. https://doi.org/10.63125/gcq1qr39

[16]. Elmoon, A. (2025b). The Impact of Human-Machine Interaction On English Pronunciation And Fluency: Case Studies Using AI Speech Assistants. *Review of Applied Science and Technology*, *4*(02), 473-500. https://doi.org/10.63125/1wyj3p84

[17]. Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, *4*(3), 224–274. https://doi.org/10.1145/501978.501980

[18]. Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategy in the impact of security breaches on firm value. *Information Systems Research*, *29*(2), 387–505. https://doi.org/10.1287/isre.2017.0749

[19]. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2008.09.005

[20]. Hozyfa, S. (2025). Artificial Intelligence-Driven Business Intelligence Models for Enhancing Decision-Making In U.S. Enterprises. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 771– 800. https://doi.org/10.63125/b8gmdc46

[21]. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems security—A survey. *IEEE Internet of Things Journal*, *4*(6), 1802–1831. https://doi.org/10.1109/jiot.2017.2703172

[22]. 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*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

[23]. Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management*, *51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.002

[24]. Jin, X., Krishnan, R., & Sandhu, R. (2012). A unified attribute-based access control model and its applications in enterprise systems. *ACM Transactions on Information and System Security*, *15*(1), 1–31. https://doi.org/10.1145/2133375.2133377

[25]. Johnson, M. E., & Goetz, E. (2007). Embedding information security into supply chain management. *International Journal of Information Security*, *6*(5), 323–331. https://doi.org/10.1007/s10207-007-0026-7

[26]. Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566. https://doi.org/10.2307/25750691

[27]. Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154. https://doi.org/10.1016/s0268-4012(02)00105-6

[28]. Khairul Alam, T. (2025). The Impact of Data-Driven Decision Support Systems On Governance And Policy Implementation In U.S. Institutions. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 994–1030. https://doi.org/10.63125/3v98q104

[29]. Knowles, W., Prince, D. D. C., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, *9*, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

[30]. Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. https://doi.org/10.17705/1jais.00232

[31]. Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

[32]. Masud, R. (2025). Integrating Agile Project Management and Lean Industrial Practices A Review For Enhancing Strategic Competitiveness In Manufacturing Enterprises. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 895–924. https://doi.org/10.63125/0yjss288

[33]. Md Arif Uz, Z., & Elmoon, A. (2023). Adaptive Learning Systems For English Literature Classrooms: A Review Of AI-Integrated Education Platforms. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 56-86. https://doi.org/10.63125/a30ehr12

[34]. Md Arman, H. (2025). Artificial Intelligence-Driven Financial Analytics Models For Predicting Market Risk And Investment Decisions In U.S. Enterprises. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1066–1095. https://doi.org/10.63125/9csehp36

[35]. Md Ismail, H. (2022). Deployment Of AI-Supported Structural Health Monitoring Systems For In-Service Bridges Using IoT Sensor Networks. *Journal of Sustainable Development and Policy*, *1*(04), 01-30. https://doi.org/10.63125/j3sadb56

[36]. Md Ismail, H. (2024). Implementation Of AI-Integrated IOT Sensor Networks For Real-Time Structural Health Monitoring Of In-Service Bridges. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *4*(1), 33-71. https://doi.org/10.63125/0zx4ez88

[37]. Md Mesbaul, H. (2024). Industrial Engineering Approaches to Quality Control In Hybrid Manufacturing A Review Of Implementation Strategies. *International Journal of Business and Economics Insights*, *4*(2), 01-30. https://doi.org/10.63125/3xcabx98

[38]. Md Mohaiminul, H. (2025). Federated Learning Models for Privacy-Preserving AI In Enterprise Decision Systems. *International Journal of Business and Economics Insights*, *5*(3), 238– 269. https://doi.org/10.63125/ry033286

[39]. Md Mominul, H. (2025). Systematic Review on The Impact Of AI-Enhanced Traffic Simulation On U.S. Urban Mobility And Safety. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 833–861. https://doi.org/10.63125/jj96yd66

[40]. Md Omar, F. (2024). Vendor Risk Management In Cloud-Centric Architectures: A Systematic Review Of SOC 2, Fedramp, And ISO 27001 Practices. *International Journal of Business and Economics Insights*, *4*(1), 01-32. https://doi.org/10.63125/j64vb122

[41]. Md Rezaul, K. (2021). Innovation Of Biodegradable Antimicrobial Fabrics For Sustainable Face Masks Production To Reduce Respiratory Disease Transmission. *International Journal of Business and Economics Insights*, *1*(4), 01–31. https://doi.org/10.63125/ba6xzq34

[42]. Md Rezaul, K. (2025). Optimizing Maintenance Strategies in Smart Manufacturing: A Systematic Review Of Lean Practices, Total Productive Maintenance (TPM), And Digital Reliability. *Review of Applied Science and Technology*, *4*(02), 176-206. https://doi.org/10.63125/np7nnf78

[43]. Md Rezaul, K., & Md Takbir Hossen, S. (2024). Prospect Of Using AI- Integrated Smart Medical Textiles For Real-Time Vital Signs Monitoring In Hospital Management & Healthcare Industry. *American Journal of Advanced Technology and Engineering Solutions*, *4*(03), 01-29. https://doi.org/10.63125/d0zkrx67

[44]. Md Rezaul, K., & Rony, S. (2025). A Framework-Based Meta-Analysis of Artificial Intelligence-Driven ERP Solutions For Circular And Sustainable Supply Chains. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 432-464. https://doi.org/10.63125/jbws2e49

[45]. Md Takbir Hossen, S., & Md Atiqur, R. (2022). Advancements In 3D Printing Techniques For Polymer Fiber-Reinforced Textile Composites: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *3*(04), 32-60. https://doi.org/10.63125/s4r5m391

[46]. Md. Hasan, I. (2025). A Systematic Review on The Impact Of Global Merchandising Strategies On U.S. Supply Chain Resilience. *International Journal of Business and Economics Insights*, *5*(3), 134–169. https://doi.org/10.63125/24mymg13

[47]. Md. Milon, M. (2025). A Systematic Review on The Impact Of NFPA-Compliant Fire Protection Systems On U.S. Infrastructure Resilience. *International Journal of Business and Economics Insights*, *5*(3), 324–352. https://doi.org/10.63125/ne3ey612

[48]. Md. Rabiul, K. (2025). Artificial Intelligence-Enhanced Predictive Analytics for Demand Forecasting In U.S. Retail Supply Chains. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 959–993. https://doi.org/10.63125/gbkf5c16

[49]. Md. Sakib Hasan, H. (2023). Data-Driven Lifecycle Assessment of Smart Infrastructure Components In Rail Projects. *American Journal of Scholarly Research and Innovation*, *2*(01), 167-193. https://doi.org/10.63125/wykdb306

[50]. Md. Sakib Hasan, H., & Abdul, R. (2025). Artificial Intelligence and Machine Learning Applications In Construction Project Management: Enhancing Scheduling, Cost Estimation, And Risk Mitigation. *International Journal of Business and Economics Insights*, *5*(3), 30–64. https://doi.org/10.63125/jrpjje59

[51]. Md. Tahmid Farabe, S. (2025). The Impact of Data-Driven Industrial Engineering Models On Efficiency And Risk Reduction In U.S. Apparel Supply Chains. *International Journal of Business and Economics Insights*, *5*(3), 353–388. https://doi.org/10.63125/y548hz02

[52]. Mohammad Shoeb, A., & Reduanul, H. (2023). AI-Driven Insights for Product Marketing: Enhancing Customer Experience And Refining Market Segmentation. *American Journal of Interdisciplinary Studies*, *4*(04), 80-116. https://doi.org/10.63125/pzd8m844

[53]. Momena, A. (2025). Impact Of Predictive Machine Learning Models on Operational Efficiency And Consumer Satisfaction In University Dining Services. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 376-403. https://doi.org/10.63125/5tjkae44

[54]. Momena, A., & Sai Praveen, K. (2024). A Comparative Analysis of Artificial Intelligence-Integrated BI Dashboards For Real-Time Decision Support In Operations. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 158-191. https://doi.org/10.63125/47jjv310

[55]. Mubashir, I. (2025). Analysis Of AI-Enabled Adaptive Traffic Control Systems For Urban Mobility Optimization Through Intelligent Road Network Management. *Review of Applied Science and Technology*, *4*(02), 207-232. https://doi.org/10.63125/358pgg63

[56]. Omar Muhammad, F. (2024). Advanced Computing Applications in BI Dashboards: Improving Real-Time Decision Support For Global Enterprises. *International Journal of Business and Economics Insights*, *4*(3), 25-60. https://doi.org/10.63125/3x6vpb92

[57]. Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization Science*, *3*(3), 398–427. https://doi.org/10.1287/orsc.3.3.398

[58]. Pankaz Roy, S. (2025). Artificial Intelligence Based Models for Predicting Foodborne Pathogen Risk In Public Health Systems. *International Journal of Business and Economics Insights*, *5*(3), 205–237. https://doi.org/10.63125/7685ne21

[59]. Pendleton, M., Garcia-Lebron, R., Cho, J.-H., & Xu, S. (2016). A survey on systems security metrics. *ACM Computing Surveys*, *49*(4), Article 53. https://doi.org/10.1145/3005714

[60]. Posey, C., Roberts, T. L., Lowry, P. B., & Bennett, R. J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of protection-motivated behaviors. *MIS Quarterly*, *37*(1), 118–A116. https://doi.org/10.25300/misq/2013/37.1.05

[61]. Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757–778. https://doi.org/10.25300/misq/2010/34.4.10

[62]. Rahman, S. M. T. (2025). Strategic Application of Artificial Intelligence In Agribusiness Systems For Market Efficiency And Zoonotic Risk Mitigation. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 862–894. https://doi.org/10.63125/8xm5rz19

[63]. Rakibul, H. (2025). The Role of Business Analytics In ESG-Oriented Brand Communication: A Systematic Review Of Data-Driven Strategies. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1096– 1127. https://doi.org/10.63125/4mchj778

[64]. Razia, S. (2022). A Review Of Data-Driven Communication In Economic Recovery: Implications Of ICT-Enabled Strategies For Human Resource Engagement. *International Journal of Business and Economics Insights*, *2*(1), 01-34. https://doi.org/10.63125/7tkv8v34

[65]. Razia, S. (2023). AI-Powered BI Dashboards In Operations: A Comparative Analysis For Real-Time Decision Support. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 62–93. https://doi.org/10.63125/wqd2t159

[66]. Reduanul, H. (2023). Digital Equity and Nonprofit Marketing Strategy: Bridging The Technology Gap Through Ai-Powered Solutions For Underserved Community Organizations. *American Journal of Interdisciplinary Studies*, *4*(04), 117-144. https://doi.org/10.63125/zrsv2r56

[67]. Reduanul, H. (2025). Enhancing Market Competitiveness Through AI-Powered SEO And Digital Marketing Strategies In E-Commerce. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 465-500. https://doi.org/10.63125/31tpjc54

[68]. Rony, M. A. (2025). AI-Enabled Predictive Analytics And Fault Detection Frameworks For Industrial Equipment Reliability And Resilience. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 705–736. https://doi.org/10.63125/2dw11645

[69]. Saba, A. (2025). Artificial Intelligence Based Models For Secure Data Analytics And Privacy-Preserving Data Sharing In U.S. Healthcare And Hospital Networks. *International Journal of Business and Economics Insights*, *5*(3), 65–99. https://doi.org/10.63125/wv0bqx68

[70]. Sabuj Kumar, S. (2025). AI Driven Predictive Maintenance in Petroleum And Power Systems Using Random Forest Regression Model For Reliability Engineering Framework. *American Journal of Scholarly Research and Innovation*, *4*(01), 363-391. https://doi.org/10.63125/477x5t65

[71]. Sadia, T. (2022). Quantitative Structure-Activity Relationship (QSAR) Modeling of Bioactive Compounds From Mangifera Indica For Anti-Diabetic Drug Development. *American Journal of Advanced Technology and Engineering Solutions*, *2*(02), 01-32. https://doi.org/10.63125/ffkez356

[72]. Sadia, T. (2023). Quantitative Analytical Validation of Herbal Drug Formulations Using UPLC And UV-Visible Spectroscopy: Accuracy, Precision, And Stability Assessment. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 01–36. https://doi.org/10.63125/fxqpds95

[73]. Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

[74]. Sai Praveen, K. (2025). AI-Driven Data Science Models for Real-Time Transcription And Productivity Enhancement In U.S. Remote Work Environments. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 801–832. https://doi.org/10.63125/gzyw2311

[75]. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, *29*(2), 38–47. https://doi.org/10.1109/2.485845

[76]. Shaikat, B. (2025). Artificial Intelligence–Enhanced Cybersecurity Frameworks for Real-Time Threat Detection In Cloud And Enterprise. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 737–770. https://doi.org/10.63125/yq1gp452

[77]. Sheratun Noor, J., Md Redwanul, I., & Sai Praveen, K. (2024). The Role of Test Automation Frameworks In Enhancing Software Reliability: A Review Of Selenium, Python, And API Testing Tools. *International Journal of Business and Economics Insights*, *4*(4), 01–34. https://doi.org/10.63125/bvv8r252

[78]. Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/10.2307/25750688

[79]. Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

[80]. Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255–276. https://doi.org/10.1287/isre.1.3.255

[81]. Syed Zaki, U. (2025). Digital Engineering and Project Management Frameworks For Improving Safety And Efficiency In US Civil And Rail Infrastructure. *International Journal of Business and Economics Insights*, *5*(3), 300–329. https://doi.org/10.63125/mxgx4m74

[82]. Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, *45*, 42–57. https://doi.org/10.1016/j.cose.2014.05.003

[83]. Tonoy Kanti, C. (2025). AI-Powered Deep Learning Models for Real-Time Cybersecurity Risk Assessment In Enterprise It Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 675–704. https://doi.org/10.63125/137k6y79

[84]. Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems*, *47*, 93–106. https://doi.org/10.1016/j.jmsy.2018.04.007

[85]. Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

[86]. Wang, Q., & Li, N. (2010). Satisfiability and resiliency in workflow authorization systems. *ACM Transactions on Information and System Security*, *13*(4), 1–35. https://doi.org/10.1145/1880022.1880023

[87]. Wells, L. J., Camelio, J. A., Williams, C. B., & White, J. (2014). Cyber-physical security challenges in manufacturing systems. *Manufacturing Letters*, *2*(2), 74–77. https://doi.org/10.1016/j.mfglet.2014.01.005

[88]. Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*(1), 4–19. https://doi.org/10.1108/09685220910944722

[89]. Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., & Terpenny, J. (2018). Cybersecurity for digital manufacturing. *Journal of Manufacturing Systems*, *48*, 3–12. https://doi.org/10.1016/j.jmsy.2018.03.006

[90]. Zhang, R., & Xu, H. (2016). Privacy concerns and online information disclosure: An integrative model and empirical test. *MIS Quarterly*, *40*(3), 569–590. https://doi.org/10.25300/misq/2016/40.3.01

[91]. Zobayer, E. (2025). Impact of Advanced Lubrication Management Systems on Equipment Longevity And Operational Efficiency In Smart Manufacturing Environments. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 618–653. https://doi.org/10.63125/r0n6bc88