Review of Applied Science and Technology

Volume: 4; **Issue:** 4
Pages: 109– 155

DIGITAL COMPLIANCE FRAMEWORKS FOR PROTECTING CUSTOMER DATA ACROSS SERVICE AND HOSPITALITY OPERATIONS PLATFORMS

Md. Towhidul Islam[1]; Rebeka Sultana[2];

[1]. *MS in Business Analytics, Trine University, USA;*
Email: towhidulislamshovan@gmail.com

[2]. *Master of Arts in Information Technology Management, Webster University, TX, USA;*
Email: rebekasultanapanna034@gmail.com

Doi: 10.63125/fp60z147
Received: *16 September 2025;* ***Revised:*** *25 October 2025;* ***Accepted:*** *17 November 2025;* ***Published:*** *29 December 2025*

Abstract

Digital compliance frameworks are essential for protecting customer data across service and hospitality operations platforms characterized by high transaction intensity, workforce turnover, and extensive system integration. This quantitative study examined the extent to which compliance framework maturity influenced customer data protection performance across service and hospitality properties, focusing on governance, process execution, and technical control layers. Property-level data were collected from 240 service and hospitality sites operating multiple customer-facing platforms. Hierarchical regression models were estimated to assess the relationships between compliance maturity and three outcome domains—compliance performance, security outcomes, and operational data handling outcomes—while controlling for property size, transaction volume, workforce turnover, geographic region, and cloud adoption level. Descriptive results indicated moderate-to-high average compliance maturity (M = 5.04, SD = 0.79 on a seven-point scale), with substantial variation across properties. Regression findings showed that compliance framework maturity explained an additional 19% of variance in audit pass performance, increasing overall explained variance to 41%. Higher compliance maturity was significantly associated with lower audit finding severity (β = −0.49, p < .001) and shorter remediation cycle times (β = −0.29, p < .001). Security-related outcomes were also affected, as compliance maturity was associated with fewer security incidents (β = −0.38, p < .001) and fewer unauthorized access events (β = −0.32, p < .001). Operational data handling outcomes demonstrated similar patterns, with maturity predicting lower policy violation rates (β = −0.44, p < .001). Moderation analysis indicated that platform ecosystem complexity and third-party dependency strengthened these relationships, accounting for an additional 4%–6% of explained variance in high-complexity environments. Comparative layer analysis revealed that governance quality had the strongest association with audit outcomes (β = 0.33), process execution showed the strongest association with operational handling outcomes (β = −0.34), and technical controls demonstrated the strongest association with security outcomes (β = −0.31). Overall, the models explained between 30% and 49% of variance across outcome categories, demonstrating that digital compliance frameworks functioned as measurable operational capabilities that significantly influenced customer data protection performance across complex service and hospitality platform ecosystems.

Keywords

Digital Compliance Frameworks, Customer Data Protection, Hospitality Platforms, Service Operations, Platform Governance.

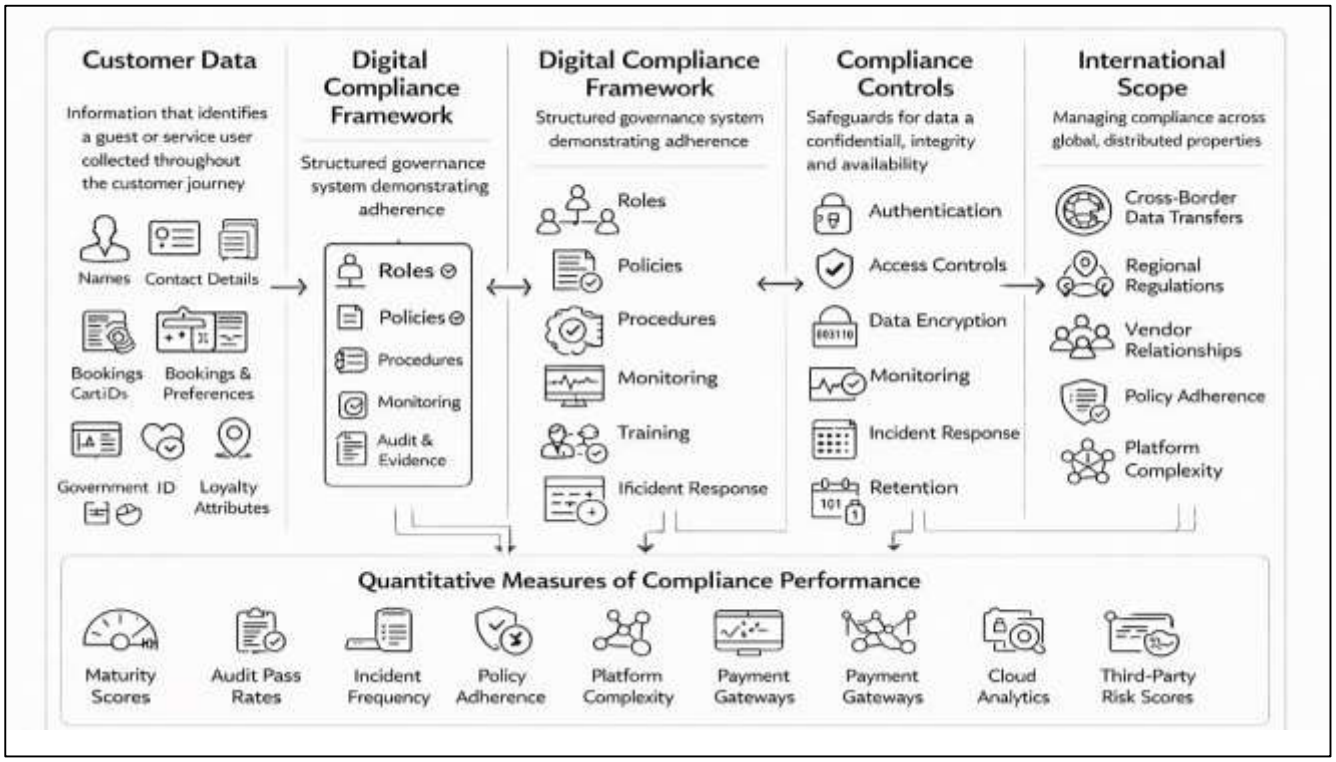
INTRODUCTION

Customer data in service and hospitality settings refers to any information that can identify, describe, relate to, or be reasonably linked with a guest or service user, including names, contact details, government identifiers, payment information, online identifiers, booking histories, loyalty attributes, location traces, preference profiles, and interaction records created through digital touchpoints across the customer journey (Line et al., 2020). Protecting customer data denotes the organized use of administrative, technical, and physical safeguards that preserve confidentiality, integrity, and availability while preventing unauthorized access, misuse, loss, alteration, or disclosure. A digital compliance framework can be defined as a structured system of governance roles, policies, standards, control objectives, operational procedures, monitoring routines, and evidence practices used to demonstrate adherence to legal requirements, industry standards, contractual obligations, and internal rules that govern the collection, processing, storage, transfer, and deletion of customer information. Within hospitality and service operations, "platforms" include property management systems, point-of-sale environments, central reservation systems, channel managers, customer relationship management tools, loyalty databases, digital identity and check-in applications, Wi-Fi onboarding portals, third-party marketplace integrations, payment gateways, and cloud analytics tools connected through APIs and data pipelines (González-Serrano et al., 2019; Jinnat & Kamrul, 2021). International significance emerges because service and hospitality ecosystems are inherently cross-border: global brands operate distributed properties, guests travel internationally, online intermediaries route bookings across countries, and cloud providers may store, replicate, or process data in multiple regions. As a result, organizations must manage multiple legal definitions of personal data, differing rules for consent and notice, distinct timelines for breach response, and varied expectations around cross-border transfers and third-party processing (Zulqarnain & Subrato, 2021). At the same time, service competitiveness depends on personalization, convenience, and seamless omni-channel delivery, which intensify both data collection and data movement across interconnected systems. A quantitative study on digital compliance frameworks therefore centers on measurable properties such as control coverage, implementation maturity, audit performance, policy adherence rates, platform configuration conformity, incident frequency, and third-party risk scores across the operational platforms that collectively handle customer data (Uddin et al., 2022; Shamim et al., 2021).

Across global markets, data protection rules and industry requirements converge on common governance principles while retaining region-specific enforcement patterns and documentation expectations. Accountability, transparency, purpose limitation, data minimization, retention discipline, and security safeguards appear repeatedly as core compliance themes, shaping how service organization's structure policy and operational control (González-Serrano et al., 2020). Hospitality organizations face additional complexity because many operate through franchising, management contracts, and shared-service models where responsibilities for data processing are distributed across corporate entities, property teams, and vendors. This distribution requires compliance frameworks that can define ownership of systems and data sets, assign decision rights for access management and vendor approvals, and establish evidence routines to show that controls are consistently implemented. The operational challenge becomes measurable when translated into organizational metrics: frequency of access reviews, onboarding and offboarding completion rates, training coverage, completeness of data inventories, documented data flows between platforms, and closure rates of audit findings (Akbar & Sharmin, 2022; Pillai et al., 2021). Digital compliance frameworks in hospitality also need to align data governance with revenue-critical processes such as reservations, payments, loyalty enrollment, and customer support. In these workflows, employees and systems interact with sensitive data under time pressure, and service quality depends on speed and reliability (Foysal & Subrato, 2022). Quantitatively, this environment can be represented through indicators of process performance and control effectiveness, such as time-to-provision access, time-to-revoke access, percentage of accounts mapped to roles, proportion of systems with encryption enabled, patch latency, and log completeness. The international scope of hospitality operations means these measures must remain comparable across properties and regions while accounting for variations in regulatory obligations, vendor contracts, and operational maturity (Kansakar et al., 2019; Zulqarnain, 2022).

Hospitality and service operations platforms generate distinctive data-protection exposure because customer data is produced at multiple touchpoints and reused across functions that span marketing, operations, and finance (Abdul, 2023; Prentice et al., 2020). Reservation and distribution components store identity, itinerary, and preference signals; property management systems extend these records with stay histories and operational notes; point-of-sale systems capture transaction details across restaurants, bars, and amenities; and loyalty platforms aggregate activity across properties and partners. Integration among these systems supports personalization and operational efficiency, yet each integration point introduces additional risks through weak authentication, misconfigured interfaces, inconsistent access control, and insufficient monitoring (Hammad & Mohiul, 2023). Operational realities amplify these risks: shift-based work encourages shared devices and fast handovers; high turnover increases the likelihood of orphaned accounts; and seasonal staffing cycles can disrupt consistent training and policy reinforcement. Many hospitality environments also include hybrid infrastructures, mixing legacy systems with cloud applications and vendor-hosted platforms, which increases heterogeneity in security capabilities and evidence collection (Choi & Kandampully, 2019; Hasan & Waladur, 2023). Payment environments add another layer of complexity because payment card handling requires strict segmentation and control rigor around cardholder data. In parallel, guest-facing digital services such as mobile check-in, digital keys, messaging, and Wi-Fi onboarding increase both the volume of data collected and the number of external services that touch guest data (Rifat & Rebeka, 2023). Quantitative research can treat these realities as measurable exposures: number of integrated vendors, volume of data-sharing relationships, count of platforms containing regulated data types, and frequency of privileged access events. These exposures shape how compliance frameworks are designed and how control performance varies across properties and platform configurations (Cheng & Jin, 2019; Kumar, 2023).

Figure 1: Digital Compliance Framework Architecture



The conceptual foundations of digital compliance frameworks in hospitality can be described through governance, control, risk, and behavioral perspectives that explain how organizations institutionalize protective routines. Governance perspectives emphasize that organizations require clear decision rights, role accountability, and standardized policies to manage complex digital ecosystems (Luo et al., 2021; Zulqarnain & Subrato, 2023). Control perspectives focus on how organizations translate policy intentions into operational practices such as access control, segregation of duties, monitoring, exception

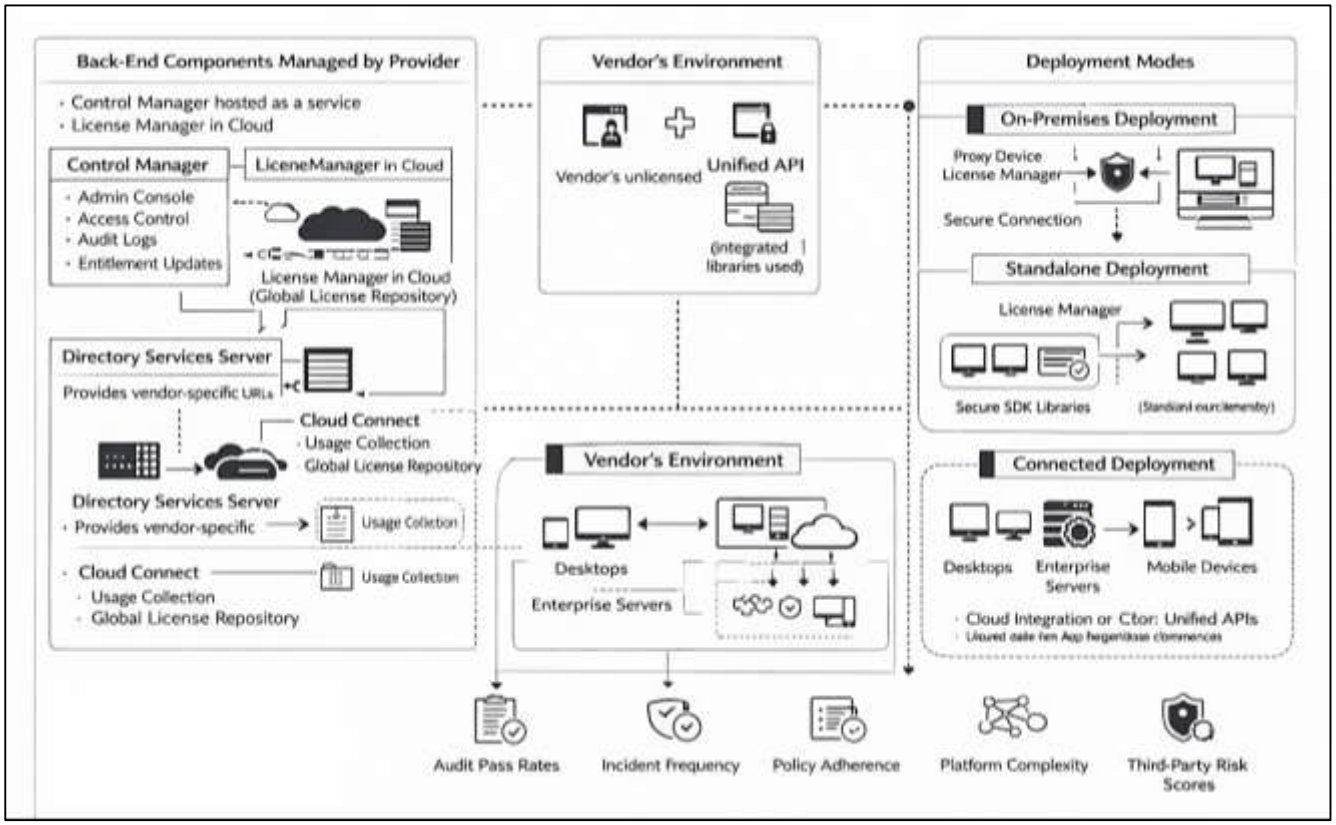
handling, and audit review. Risk perspectives define compliance as a structured response to uncertainty and potential loss, emphasizing inventory, assessment, treatment, and continuous oversight across platforms and vendors. Behavioral perspectives highlight that a significant portion of compliance performance depends on employee actions, including secure handling of customer information, correct system use, avoidance of workarounds, and timely incident reporting. Hospitality settings intensify behavioral variability because work is fast-paced, customer-facing, and distributed across many locations and roles (Li et al., 2022; Masud & Hossain, 2024). Quantitatively, these foundations allow compliance frameworks to be measured not only by the presence of controls but also by their execution: training completion and comprehension, rates of policy exception, frequency of improper access attempts, and adherence to data handling routines at service points. These theoretical foundations also support modeling how organizational design elements—leadership engagement, clarity of policies, usability of security measures, and availability of support—relate to measurable compliance outcomes (Lai, 2019). By grounding the study in constructs that can be operationalized, a quantitative approach avoids ambiguous or purely descriptive assessments and enables structured comparison across brands, properties, or platform ecosystems.

Digital compliance frameworks are typically implemented through layered architectures that connect governance structures to process workflows and technical controls. At the governance layer, organizations define privacy and security roles, establish policies for acceptable use and data handling, maintain system and data inventories, and set control objectives mapped to internal standards and external requirements (Lee, 2019; Md & Praveen, 2024). At the process layer, frameworks specify routines for identity lifecycle management, role-based access design, privileged access approval, vendor onboarding and periodic reassessment, incident triage, breach reporting escalation, and rights request handling. At the technical layer, controls include encryption, tokenization for payment data, network segmentation, multi-factor authentication, secure configuration baselines, vulnerability management, endpoint security, logging, and continuous monitoring. Because hospitality operations platforms often integrate with third parties, frameworks also include contractual and monitoring controls for service providers, such as documented processing responsibilities, data-sharing constraints, and evidence of security practices (Kim & Kim, 2022; Nahid & Bhuya, 2024). A quantitative study can operationalize these layers as measurable categories. Governance can be scored through policy coverage and role assignment completeness. Process can be measured through frequency and timeliness of reviews, training coverage, and documented exceptions. Technical posture can be quantified through configuration compliance rates, patching speed, encryption coverage, and monitoring completeness (Font et al., 2021; Newaz & Jahidul, 2024). The layered view supports statistical analysis because it enables clear variable construction and facilitates identification of which layer explains more variance in compliance performance across properties and platform setups.

Operationalizing "protecting customer data" for quantitative analysis requires clear constructs, consistent measurement, and stable units of observation across hospitality organizations (Seo & Lee, 2021). Customer data protection can be represented using metrics tied to confidentiality, integrity, and availability outcomes: number of unauthorized access events, rate of high-risk vulnerabilities, frequency of misconfigurations in critical systems, incident counts, detection and containment times, and severity-weighted audit findings (Akbar, 2024; Zhao et al., 2019). Compliance performance can be quantified using maturity indices, control coverage scores, audit pass rates, remediation cycle times, and evidence completeness for required documentation. Privacy governance can be captured through metrics such as retention compliance rates, deletion request cycle times, completeness of data flow maps, and proportion of systems with documented lawful processing bases or internal approvals. Human-factor compliance can be measured using survey-based scales for policy adherence and awareness, complemented by behavioral telemetry such as training completion, phishing simulation performance, and rates of access policy violations (Buhalis & Sinarta, 2019). Platform complexity can be quantified through number of interconnected applications, number of vendors with data access, volume of API connections, and the count of data repositories holding regulated data categories. Cross-border exposure can be measured through number of jurisdictions represented in guest profiles, number of international transfers, and reliance on globally distributed cloud hosting arrangements. These operational definitions allow the quantitative model to connect framework design and execution

to measurable outcomes without relying on narrative claims. The resulting research design can examine associations among framework maturity, platform complexity, third-party exposure, and measured protection outcomes across service and hospitality operations platforms (Park, 2020).

Figure 2: Digital Compliance Framework Architecture



The objective of this quantitative study is to measure and explain how digital compliance frameworks protect customer data across service and hospitality operations platforms by examining the relationships among framework maturity, control coverage, platform integration complexity, third-party data sharing, and measurable data-protection performance outcomes within hotels, restaurants, resorts, and other service-intensive venues. Specifically, the study aims to (a) operationalize "digital compliance framework maturity" as a multidimensional construct that captures governance completeness (role assignment, policy scope, accountability routines), process execution (access lifecycle management, training coverage, incident handling procedures, retention and deletion practices), and technical control implementation (encryption coverage, authentication strength, logging and monitoring completeness, patch and vulnerability management), (b) quantify "platform exposure" through the number and type of interconnected operational systems such as property management systems, point-of-sale systems, central reservation systems, customer relationship management tools, loyalty platforms, Wi-Fi onboarding portals, mobile check-in applications, and analytics or marketing automation tools, (c) quantify "third-party risk scope" through the count of external vendors and marketplaces with customer-data access, the intensity of data exchange via APIs, and documented data-sharing relationships, and (d) model "customer data protection performance" using observable indicators including security audit results, control test pass rates, remediation cycle times for identified weaknesses, frequency of unauthorized access events, incidence counts of data-handling violations, and time-based measures for detection and containment of security incidents . The study also aims to compare whether properties or business units with higher compliance maturity demonstrate more consistent control execution and stronger protection outcomes even when operating under high integration complexity and extensive vendor ecosystems. In doing so, the research will identify which layers of compliance frameworks—governance, process, or technical controls—explain the greatest variation in protection performance across operational contexts, and whether certain platform

configurations (for example, highly integrated reservation-to-payment workflows or heavy reliance on third-party booking channels) are associated with greater compliance burden and higher exposure. Finally, the study seeks to produce a replicable measurement approach that allows organizations to benchmark compliance implementation across properties and platforms using standardized metrics, enabling statistically grounded comparisons across service and hospitality environments where customer data is continuously collected, transferred, and utilized for operational delivery.

LITERATURE REVIEW

The literature review for this quantitative study synthesizes scholarship on digital compliance frameworks, customer data protection, and the operational realities of service and hospitality technology platforms (Couclelis, 2020). Because hospitality and service organizations rely on interconnected systems—such as property management systems, point-of-sale platforms, reservation and distribution tools, customer relationship management applications, loyalty databases, payment gateways, and vendor-integrated cloud services—customer data is continuously created, transferred, stored, and reused across multiple technical and organizational boundaries. This operational architecture increases exposure to privacy violations, unauthorized access, misconfigurations, and third-party risks, making compliance frameworks central to how organizations structure governance, implement controls, and demonstrate accountability in routine operations. The review therefore focuses on empirical and conceptual work that explains how compliance programs are built, what control categories they typically include, and which measurable conditions affect control performance across multi-platform environments (Walsh & Rowe, 2023). In alignment with the quantitative nature of the paper, the literature review emphasizes constructs and indicators that can be operationalized into variables, such as compliance maturity, control coverage, audit performance, access management quality, incident frequency, integration complexity, and vendor data-sharing intensity. The section also organizes prior research into a coherent model-building foundation by linking compliance governance, technical safeguards, process execution, and human behavioral adherence to measurable outcomes that represent the strength of customer data protection. Rather than presenting broad generalities, the review is structured to identify which dimensions of compliance frameworks have demonstrated measurable associations with privacy and security performance, and how the service/hospitality context introduces unique moderating conditions such as high staff turnover, shift-based device usage, distributed properties, and frequent dependence on external platforms and intermediaries (Wiig et al., 2020).

Customer Data in Hospitality

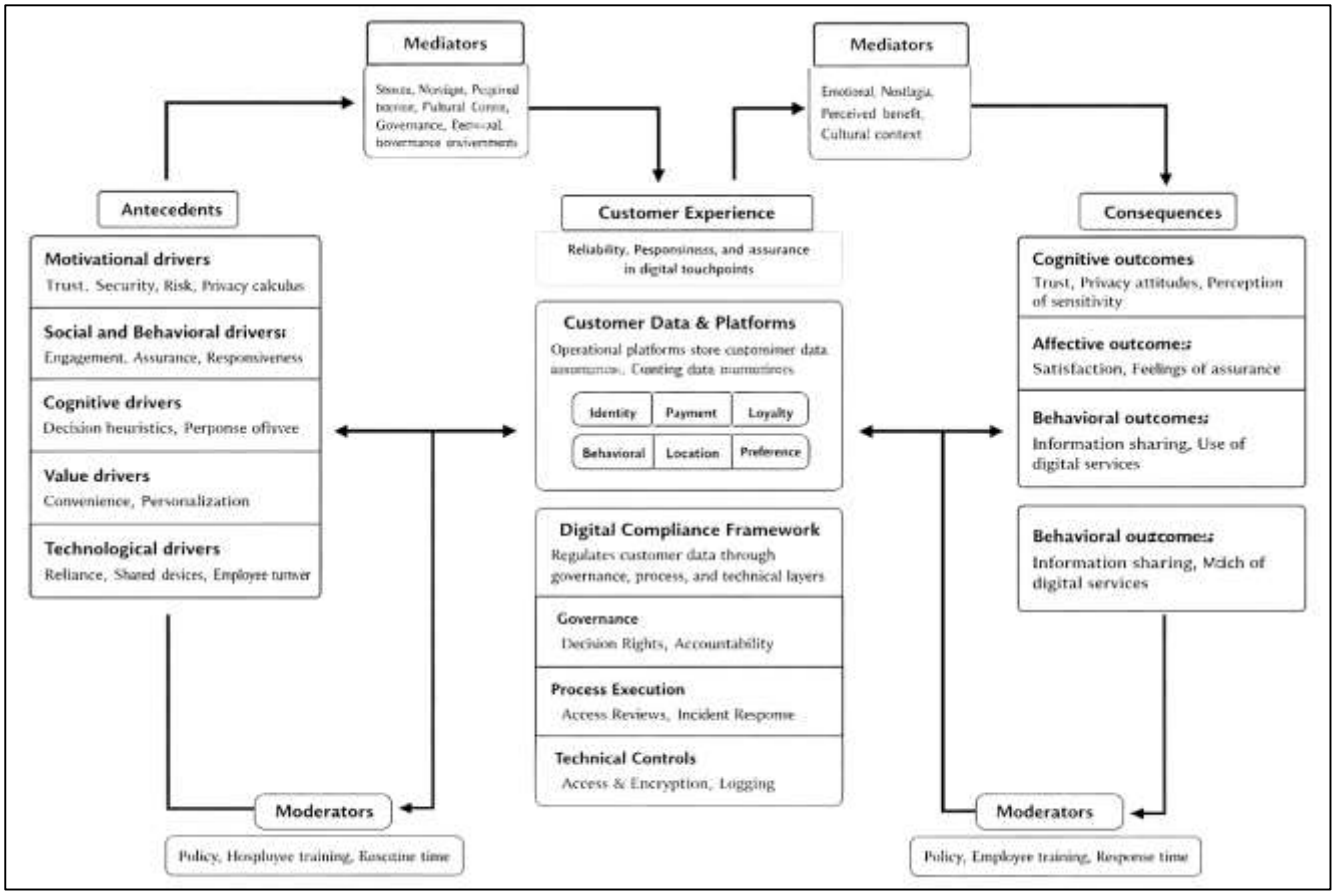
Customer data in hospitality and service resulting from digital interactions can be defined as recorded information that identifies a guest or service user, describes their transactions, or captures contextual details about their preferences and behaviors across service touchpoints (Badi & Murtagh, 2019). Across hotels, restaurants, resorts, and multi-site service venues, customer data is commonly grouped into identity data (names, contact details, government identifiers used for check-in), payment data (card-related details, billing tokens, transaction confirmations), loyalty data (membership identifiers, points histories, tier status, partner accruals), behavioral and interaction data (service requests, complaint logs, clickstream activity in mobile apps, chat transcripts), location data (property presence, Wi-Fi association, venue check-ins), and preference profiles (room choices, dietary restrictions, language preferences, accessibility needs). Research on information privacy and consumer trust indicates that customers view these categories differently in terms of sensitivity and acceptable use, and that perceived misuse or poor handling can weaken willingness to engage with digital service features (Aase & Waring, 2020; Rabiul & Alam, 2024). Work on privacy calculus and disclosure behavior shows that individuals assess perceived benefits relative to perceived risks when deciding whether to share information in technology-mediated services, which is especially relevant in hospitality where personalization and convenience are marketed as value propositions. Services and digital service quality research also emphasizes that customer experience is shaped by reliability, responsiveness, and assurance in digital channels, and data protection behaviors contribute directly to assurance perceptions at critical moments such as booking, payment, and identity verification. For a quantitative study that needs comparable measurements across diverse properties and platforms, a practical boundary-setting approach is to treat customer data as the set of information elements stored or

processed by operational platforms that support the service encounter and the commercial transaction. A measurable mapping approach can be built by classifying each platform according to which categories of customer data it stores or processes, then using that classification to represent relative sensitivity as a structured index that reflects how many regulated or high-risk categories appear in the platform's data footprint. The unit of analysis is consequential in hospitality research because operations can be centrally governed at the brand level while execution varies at the property level, and customer data is also partitioned by platforms that may be shared across multiple properties. Property-level analysis aligns with operational realities such as staffing practices, device usage, local compliance execution, and incident response behaviors (Pluchinotta et al., 2022; Kumar, 2024). Brand-level analysis captures governance decisions, vendor selection, standardized policies, and centralized security tooling. Platform-level analysis supports control testing and configuration measurement because the platform is where controls are implemented and where logs provide evidence of access, changes, and anomalies. Together, these definitions and boundaries position customer data protection as a measurable operational phenomenon rather than a purely legal or conceptual topic, enabling quantitative research designs that compare how data categories and operational contexts shape compliance requirements and protection performance across hospitality and service ecosystems.

A digital compliance framework can be defined as an organized, auditable system that translates external obligations and internal rules into enforceable governance structures, repeatable operational processes, and technical safeguards for customer data across service operations platforms. The governance dimension typically includes role assignment, decision rights, policy architecture, accountability routines, and documentation practices that allow an organization to demonstrate control ownership and oversight (Praveen, 2024; Singh & Aggarwal, 2022). Governance research in information systems and security has long emphasized that policy existence alone is insufficient; effectiveness depends on clarity of responsibility, alignment with business decision rights, and routine oversight that produces evidence. Within hospitality organizations, governance often spans corporate security leadership, privacy or compliance leadership, platform owners, property-level managers, and vendor management functions. The process execution dimension refers to how governance requirements are operationalized through standard routines, such as identity lifecycle management for employees and contractors, role-based access design, periodic access reviews, workforce training and acknowledgment, incident reporting and triage procedures, retention and deletion workflows, and vendor onboarding and reassessment. Behavioral information security research supports the view that policy compliance is shaped by deterrence perceptions, normative influence, and the usability of the prescribed behaviors; this is salient for hospitality where work is fast-paced, service-facing, and frequently staffed with rotating shifts. Process execution therefore becomes a measurable domain through indicators that reflect how consistently required steps occur, how quickly access changes are completed, and how reliably incidents are escalated through defined channels (Shams et al., 2021; Azam & Amin, 2024). The technical controls dimension covers the safeguards deployed in platforms and infrastructure that store or transmit customer data, including strong authentication, multi-factor access for privileged functions, encryption for stored and transmitted data, logging and monitoring coverage, secure configuration baselines, patch and vulnerability management practices, and network segmentation for sensitive environments such as payment processing. Security engineering and risk management scholarship underscores that technical controls must be integrated into operational workflows so that protections remain effective under real-world conditions, and that continuous monitoring is essential to detect misuse and configuration drift. For quantitative research, a measurable system definition supports constructing a maturity representation that reflects the completeness and execution quality of governance, process, and technical elements. Such a maturity construct can be designed to represent how comprehensively a hospitality organization defines responsibilities, implements repeatable routines, and deploys enforceable controls across platforms. This approach aligns with measurement traditions in governance and compliance research that compare organizational control environments using structured indicators, and it supports platform-by-platform evaluation of customer data protection practices (Hammad & Hossain, 2025; Steenberg et al., 2019). In hospitality settings where properties may vary in staffing stability and local operational discipline, and where brands may vary in centralization and vendor strategies, defining the compliance framework as

a measurable system establishes a consistent analytical foundation for comparing protection capability across operational contexts without relying on purely descriptive assessments.

Figure 3: Digital Compliance Conceptual Framework



Service and hospitality operations platforms form a data ecosystem because customer information flows across multiple systems that collectively support discovery, booking, check-in, service delivery, payment, and post-stay engagement (Borie et al., 2021; Mosheur, 2025). Property management systems act as operational cores for room allocation and stay records; point-of-sale systems record purchases across outlets; central reservation systems and distribution tools coordinate booking inventory and customer identifiers; customer relationship management platforms store profiles and engagement history; loyalty systems link identities to long-term value programs; Wi-Fi onboarding portals and guest engagement tools capture device and interaction information; mobile check-in and digital key applications extend identity and authentication flows; and analytics and marketing tools aggregate behavioral signals for segmentation and personalization (Kumar, 2025). Tourism and hospitality information systems research documents that digitization has increased the interconnectedness of these systems and expanded reliance on external intermediaries, including booking channels, payment processors, and cloud-based service providers. Platform ecosystems support operational efficiency and customer convenience, yet platform complexity introduces practical compliance challenges because controls must be consistent across many systems, interfaces, and organizational boundaries. Cybersecurity and threat landscape research emphasizes that integration points and third-party dependencies can broaden attack surfaces, while breach-focused work highlights that adversary may exploit weaker systems, misconfigurations, or supplier relationships to gain access to sensitive data (Hamzei et al., 2020; Zaheda, 2025b). From a service operations perspective, the hospitality environment adds structural conditions that can influence platform security and compliance: distributed properties with varying local capability, high employee turnover that can disrupt access governance, shared devices and shift handovers that increase the risk of credential misuse, and time pressure at service counters that can motivate workarounds. Digital service quality research supports

the importance of maintaining reliability and assurance across digital touchpoints, suggesting that protective controls must be implemented in ways that do not undermine operational continuity. For quantitative study design, the ecosystem view enables measuring integration exposure by documenting the number of systems involved in customer data processing, the number of integrations between systems, and the breadth of vendor connections that exchange data. Integration exposure is not merely a technical concept; it can be linked to operational governance demands such as coordinating policies across platform owners, aligning configuration standards, and ensuring auditability across systems managed by different teams or vendors. When the platform ecosystem is treated as the empirical context for compliance, the literature suggests that data protection is best understood as the combined performance of controls across connected systems rather than as the performance of a single application (Hultin, 2019; Zaheda, 2025a). This framing supports quantitative comparisons across properties or brands that differ in digitization depth, vendor dependency, and standardization, and it creates a basis for analyzing how platform ecosystem characteristics relate to observable compliance outcomes, such as audit findings, policy violations, and incident occurrence patterns.

Rewriting the variable mapping concepts without formulas, the literature supports representing platform complexity and data sensitivity as structured classifications that translate operational realities into comparable quantitative indicators. Data sensitivity can be represented by identifying which categories of customer data are present within each operational platform and then describing sensitivity in terms of the breadth of regulated or high-risk categories held or processed (Petersen & Kruss, 2021). This mapping approach is consistent with privacy and governance scholarship that emphasizes data inventories, data classification, and data flow documentation as prerequisites for accountability and control testing. Similarly, platform integration complexity can be represented by documenting how many operational systems participate in the customer data lifecycle and how extensively those systems exchange data through interfaces and vendor connections. This can be captured through counts of connected systems, documented integration relationships, and the presence of external intermediaries that process customer information, producing a structured representation of integration exposure. Governance and security management research indicates that as organizational systems become more interconnected, effective compliance increasingly depends on consistent decision rights, cross-functional coordination, and evidence-producing routines that operate across platforms. Behavioral security studies add that the human dimension becomes more challenging in complex environments, because employees must navigate multiple systems under time pressure while maintaining secure practices. In hospitality, operational dispersion and workforce dynamics may increase variance in how policies are followed at the property level, even when brand-level governance is standardized. Therefore, the literature supports boundary choices that align with the research question: property-level analysis captures local execution of access control, training, and incident reporting; brand-level analysis captures centralized governance, vendor standards, and audit programs; and platform-level analysis captures technical control deployment and measurable configuration states (Senyo et al., 2019). A literature-grounded quantitative framing can also distinguish between controls that are primarily organizational, such as policy governance and accountability routines, controls that are procedural, such as access reviews and retention workflows, and controls that are technical, such as encryption, authentication strength, logging coverage, and segmentation. Treating these as separate but related dimensions aligns with established views of security governance that emphasize the need for coordinated layers rather than single-control solutions. In this way, the constructs become specific enough to support statistical modeling while remaining operationally meaningful for service and hospitality platforms that must handle customer data across multiple systems, properties, and vendor relationships. This construct clarity also supports coherent literature review synthesis because it allows prior studies on privacy trust, governance, security controls, risk management, and service operations digitization to be organized around measurable domains that map to real operational practices within hospitality technology ecosystems (Wankmüller & Reiner, 2020).

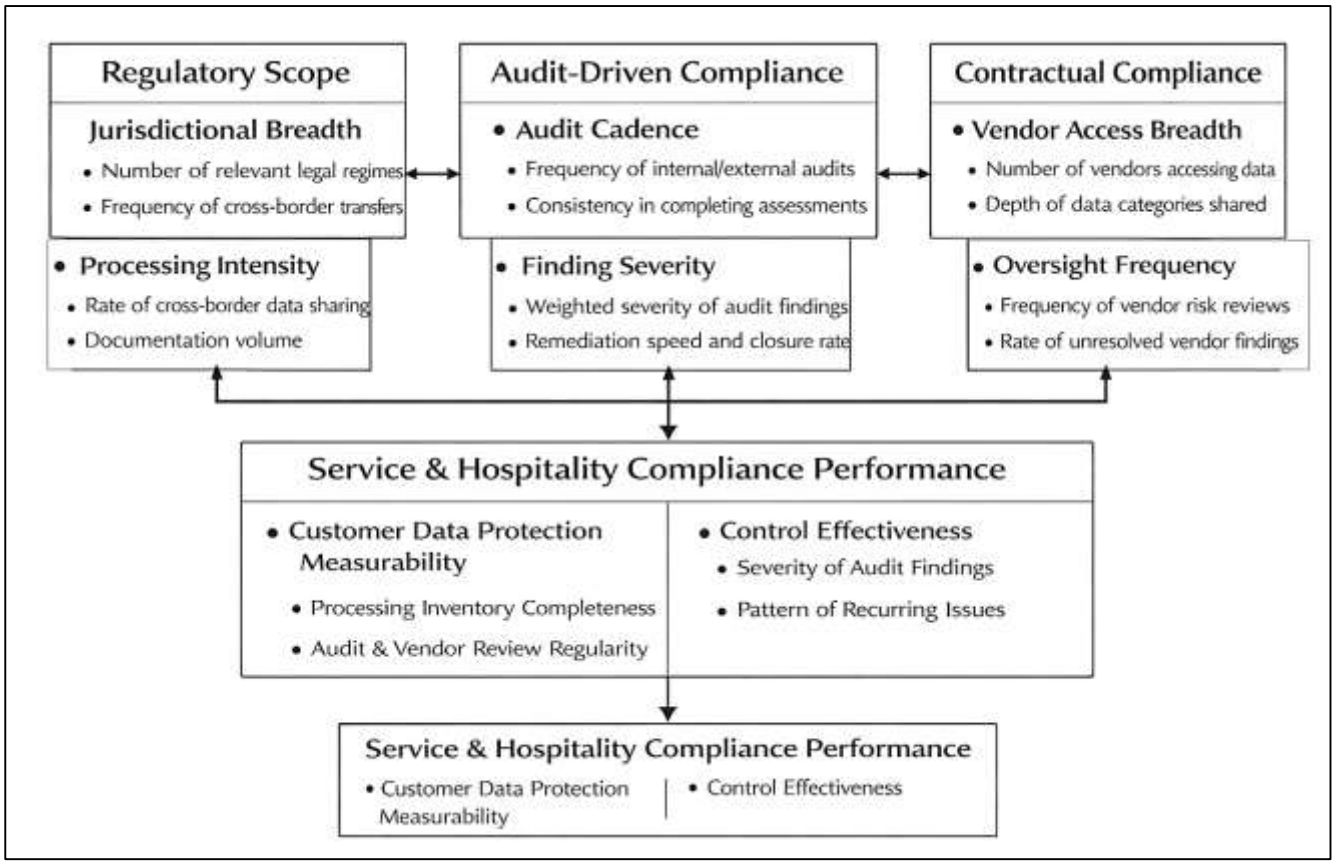
Compliance Drivers

Regulatory obligations operate as measurable scope pressure in service and hospitality because customer data routinely crosses organizational and national boundaries through travel patterns, multinational brand footprints, online booking intermediaries, and cloud hosting arrangements. The literature on global privacy governance characterizes modern compliance as a multi-regime coordination problem in which organizations must align internal practices with overlapping legal expectations related to notice, lawful processing, consumer rights, breach reporting, and accountability documentation across jurisdictions (Zhang et al., 2019). In hospitality, this scope pressure is intensified by business models that combine centralized brand operations with distributed properties, each collecting identity, payment, and preference information under locally situated workflows. A quantitative framing treats regulatory scope as an observable environmental condition rather than an abstract legal backdrop by counting how many distinct jurisdictions are materially relevant to an organization's operations and customer base and by tracking how often customer data is transferred across borders through platform integrations, vendor processing, or centralized corporate systems. Research on transborder data flows emphasizes that cross-border exposure increases compliance complexity because organizations must determine legal transfer bases, establish governance for data localization or hosting choices, and maintain documentation that connects specific data flows to legitimate processing purposes (Beach et al., 2020). Accountability-focused scholarship also shows that regulatory scope pressure manifests operationally through the expansion of documentation, monitoring, and reporting duties, which can be measured through the volume and completeness of records needed for audits, assessments, and rights request handling. In hospitality settings, regulatory scope is not limited to privacy law alone; consumer protection obligations, payment regulations, and sectoral security expectations frequently intersect with privacy governance in the same operational platforms. A measurable approach therefore aligns with the literature by representing scope pressure through structured indicators that capture the breadth of legal regimes relevant to the organization's guest journeys and the operational frequency with which customer data moves beyond national boundaries. This framing supports quantitative comparisons across firms that primarily serve domestic guests and host data locally versus firms that serve international travelers and rely heavily on cross-border processing through global platforms (Fuchs et al., 2020). It also supports property-level and brand-level analysis by allowing researchers to examine whether increases in regulatory scope are associated with higher compliance maturity, more frequent control testing, and stronger audit documentation practices in hospitality operations.

Industry standards and audit-driven compliance are widely treated in the literature as mechanisms that translate broad regulatory expectations into actionable control requirements and verifiable assurance routines, particularly in payment-heavy service environments (Fasoulis & Kurt, 2019). Hospitality operations frequently process payment data through point-of-sale systems, payment gateways, and reservation engines, creating a compliance context where payment security requirements drive the adoption of prescriptive technical and operational controls, including secure configurations, access restrictions, logging, and monitoring practices that can be tested through audits. Security management standards also function as organizational coordination tools by providing a structured approach for establishing policies, defining roles, conducting risk assessments, and maintaining evidence of control operation across distributed environments. Within services research, audit regimes are often described as institutional instruments that shape organizational behavior through external scrutiny and formalized assessment cycles, which is especially relevant in hospitality where properties vary in local capability and staffing stability. A quantitative perspective can represent audit-driven compliance through observable characteristics such as how often internal or external audits occur, how consistently properties complete assessments on schedule, and how severe the resulting findings are when rated by predefined criteria (Burdon & Sorour, 2020). Severity-weighted findings are particularly useful in hospitality contexts because the same number of findings can represent vastly different risk postures depending on whether issues relate to minor documentation gaps or material control failures affecting payment or identity systems. The literature on information security governance and risk management supports measuring audit outcomes as indicators of both control effectiveness and organizational discipline, because audits capture not only whether controls

exist but whether they are functioning and documented. This aligns with the operational reality that hospitality platforms are frequently updated, integrated, and reconfigured, creating ongoing potential for control drift that periodic audits can detect. Audit-driven compliance also intersects with service quality research because controls must operate without disrupting revenue processes such as check-in, payment authorization, and guest communications, creating measurable tensions between operational speed and assurance routines that can be captured through remediation timelines and closure rates of findings (Malola & Maroun, 2019). By structuring audit frequency and finding severity as quantifiable indicators, the literature supports empirical tests of whether properties with more regular audit cycles and stronger closure discipline demonstrate more consistent compliance execution across their operational platforms.

Figure 4: External Compliance Drivers in Hospitality



Contractual compliance and vendor responsibility allocation are central compliance drivers in hospitality because customer data is frequently processed by third parties that provide booking distribution, cloud hosting, marketing automation, identity verification, payment processing, analytics, customer messaging, and managed security services (Waxin et al., 2019). The literature on privacy governance and organizational accountability emphasizes that compliance obligations persist even when processing is outsourced, requiring organizations to define responsibilities, monitor vendor performance, and maintain evidence that vendors meet required safeguards. Hospitality's platform ecosystem amplifies this dynamic because properties may depend on vendor-managed systems for core operational functions, while corporate teams may oversee vendor selection and contracting, resulting in shared responsibility patterns that must be operationalized into enforceable terms and measurable oversight routines. Vendor responsibility allocation can be represented in quantitative research by documenting where customer data processing occurs (internally managed systems versus vendor-managed platforms), the number of vendors with access to customer data, and the breadth of data types shared with each vendor. This approach reflects supply-chain and outsourcing research showing that risk exposure increases as more external entities touch sensitive information and as data-sharing relationships become more complex and less transparent (Rhodes et al., 2021). Risk

management scholarship also supports measuring third-party exposure through structured inventories and due diligence evidence, because vendor risk is shaped by both the number of relationships and the depth of access those vendors have to sensitive categories such as identity and payment information. In hospitality, contractual compliance frequently includes requirements related to breach notification cooperation, access controls, incident response coordination, and limitations on subcontracting, all of which can be represented through measurable contract clause coverage and oversight frequency. The literature on institutional compliance further explains why contracts and attestations often become operational substitutes for direct control, driving organizations toward routine assessments, standardized questionnaires, and third-party assurance reports that can be quantified as part of vendor governance. This creates a measurable operational footprint: frequency of vendor reviews, completeness of vendor risk documentation, rate of unresolved vendor findings, and alignment between vendor-provided evidence and internal control requirements (Borsatto & Bazani, 2021). Such measures reflect the practical reality that hospitality organizations must maintain compliance across a mosaic of internal and vendor-managed platforms that collectively shape the protection of customer data.

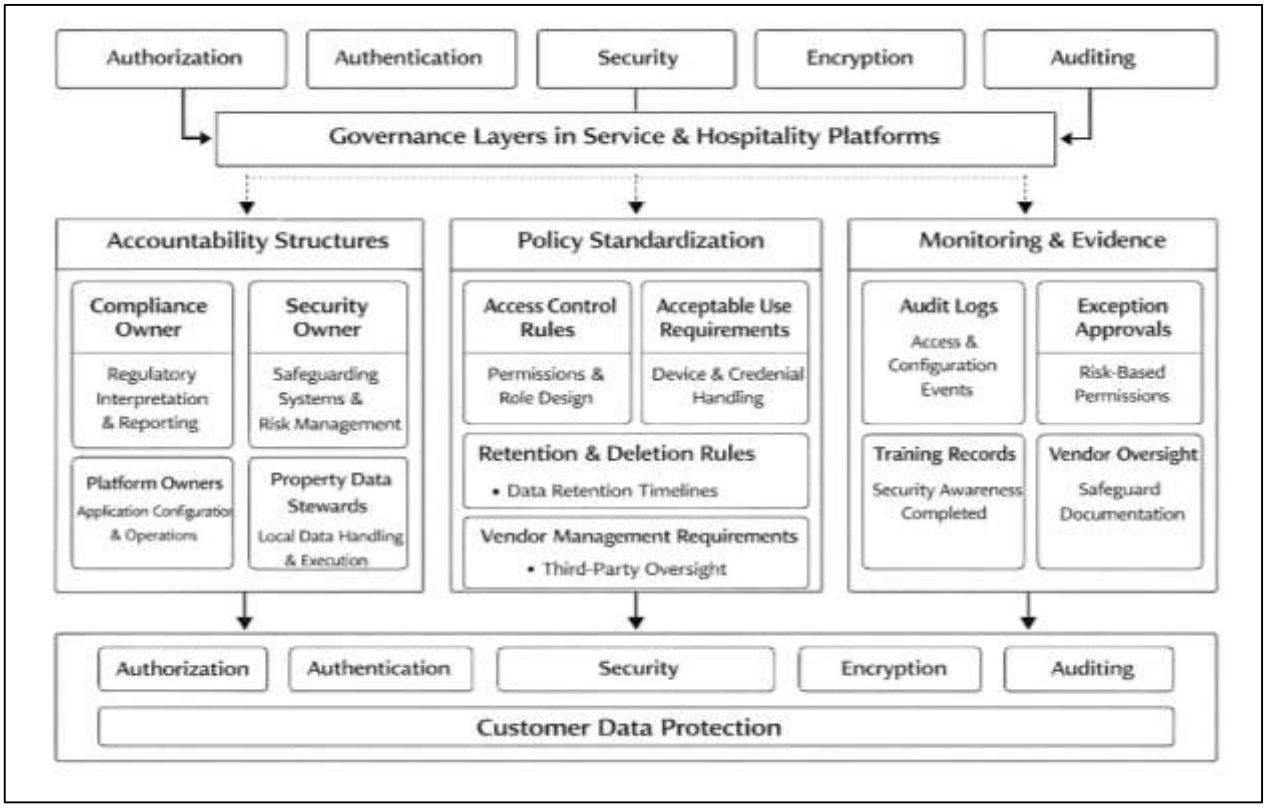
Synthesizing these compliance drivers, the literature supports a quantitative view in which regulation, standards, and contracts function as external governance pressures that shape the scope, rigor, and measurability of compliance programs across service and hospitality operations platforms. Regulatory breadth increases the documentation and control requirements tied to cross-border guest journeys and data transfers, creating quantifiable differences in compliance workload and monitoring needs across organizations (Ariono et al., 2022). Standards and audits convert broad obligations into structured control expectations and assurance cycles, enabling measurable comparisons through audit cadence, severity-weighted findings, remediation speed, and closure discipline. Contractual compliance and vendor responsibility allocation extend these pressures into the supply chain, where third-party access becomes a measurable driver of exposure and a determinant of oversight intensity. Across these drivers, a consistent empirical theme is that compliance is not solely a legal state; it is an operational capability expressed through routines that can be counted, tested, scored, and compared across properties and brands. Hospitality research on technology ecosystems reinforces that compliance performance depends on how well organizations coordinate controls across interconnected platforms, particularly when payment processing, reservations, and guest engagement systems are integrated with external providers (Danese et al., 2019). Governance and risk scholarship further emphasizes that accountability requires demonstrable evidence, which aligns with measurable indicators such as the completeness of processing inventories, the regularity of audits and vendor reviews, and the severity patterns of recurring findings. A literature-grounded quantitative structure therefore treats jurisdictional reach and cross-border processing intensity as scope indicators, audit cadence and finding severity as assurance indicators, and vendor access breadth as supply-chain exposure indicators. This structure is consistent with established approaches in privacy governance, security management, and institutional compliance research and provides a coherent basis for modeling how external compliance drivers relate to observable control performance and customer data protection outcomes across hospitality operations platforms (Potter et al., 2019).

Governance Layer of Compliance Frameworks

Accountability structures and role clarity form the core governance foundation of digital compliance frameworks in service and hospitality operations because customer data protection spans multiple organizational layers, technical domains, and operational contexts (Zhang et al., 2023). In hospitality environments, customer data is handled by front-desk staff, food and beverage teams, IT administrators, marketing units, finance departments, and external service providers, all of whom interact with different systems and data categories. Governance literature consistently emphasizes that effective compliance depends on explicit assignment of responsibility rather than diffuse or assumed ownership. Within hospitality organizations, accountability is typically distributed across clearly defined roles such as a compliance owner who coordinates regulatory interpretation and reporting, a security owner responsible for safeguarding systems and managing risk exposure, platform owners accountable for configuring and operating specific applications that process customer data, and property-level data stewards who oversee local execution of data handling practices. These roles

anchor compliance activities in identifiable individuals or teams, enabling consistent decision-making around access approvals, exception handling, incident escalation, and vendor coordination. Role clarity reduces ambiguity in operational settings where rapid service delivery can otherwise override governance considerations, particularly during high-volume periods such as peak travel seasons or large events (Bhavsar et al., 2023). Organizational governance research also shows that when responsibilities are clearly defined, monitoring activities become more effective because deviations can be traced back to accountable owners rather than remaining unresolved due to unclear authority. In hospitality, where properties often operate semi-autonomously under brand standards, role clarity also supports alignment between corporate governance expectations and property-level execution by establishing clear reporting lines and escalation pathways. From a quantitative perspective, accountability structures can be represented through observable indicators such as the presence of formally documented roles, consistency of role assignment across properties, clarity of escalation procedures, and the extent to which responsibilities for data protection tasks are explicitly mapped to specific owners. These characteristics allow governance capability to be examined empirically rather than descriptively, positioning accountability as a measurable attribute of compliance maturity across service and hospitality operations platforms (Jiménez et al., 2020).

Figure 5: Governance Layers for Data Protection



Policy architecture and standardization across properties represent a second governance mechanism that operationalizes accountability into enforceable rules guiding how customer data is handled in everyday service delivery (Zhao & Wang, 2019). Policies define acceptable and unacceptable behaviors, establish minimum control expectations, and provide a reference point for training, monitoring, and enforcement. In hospitality operations, core policy domains commonly include access control rules governing who may access customer data and under what conditions, acceptable use requirements addressing device and credential handling, retention and deletion rules defining how long customer data may be stored and how it must be disposed of, incident response procedures specifying detection and escalation steps, and vendor management requirements outlining due diligence and oversight expectations for third parties. Governance research emphasizes that policy effectiveness depends on standardization across organizational units, especially in distributed environments where local

practices can diverge in the absence of clear guidance. In hospitality, standardized policies help ensure that the same data protection expectations apply across properties that may differ significantly in size, staffing stability, and technical capability (Malik et al., 2023). Policy standardization also supports centralized oversight by enabling corporate teams to assess compliance using consistent criteria rather than negotiating property-specific interpretations. At the same time, operational literature highlights those policies must be sufficiently specific and current to remain relevant to rapidly evolving platform ecosystems that integrate cloud services, mobile applications, and third-party tools. Policies that lag behind operational reality can create gaps between documented expectations and actual system behavior. From a measurement standpoint, policy architecture can be represented through indicators reflecting the breadth of policy coverage across relevant domains and the discipline with which policies are reviewed and updated to reflect platform changes, new integrations, or revised operational workflows. These indicators capture governance quality by assessing whether organizations maintain a living policy framework that actively guides platform configuration and employee behavior rather than a static set of documents disconnected from daily operations (Geldenhuys et al., 2021). In hospitality settings, policy standardization thus functions as a governance bridge that translates abstract compliance requirements into consistent operational rules across all customer-facing and back-office platforms.

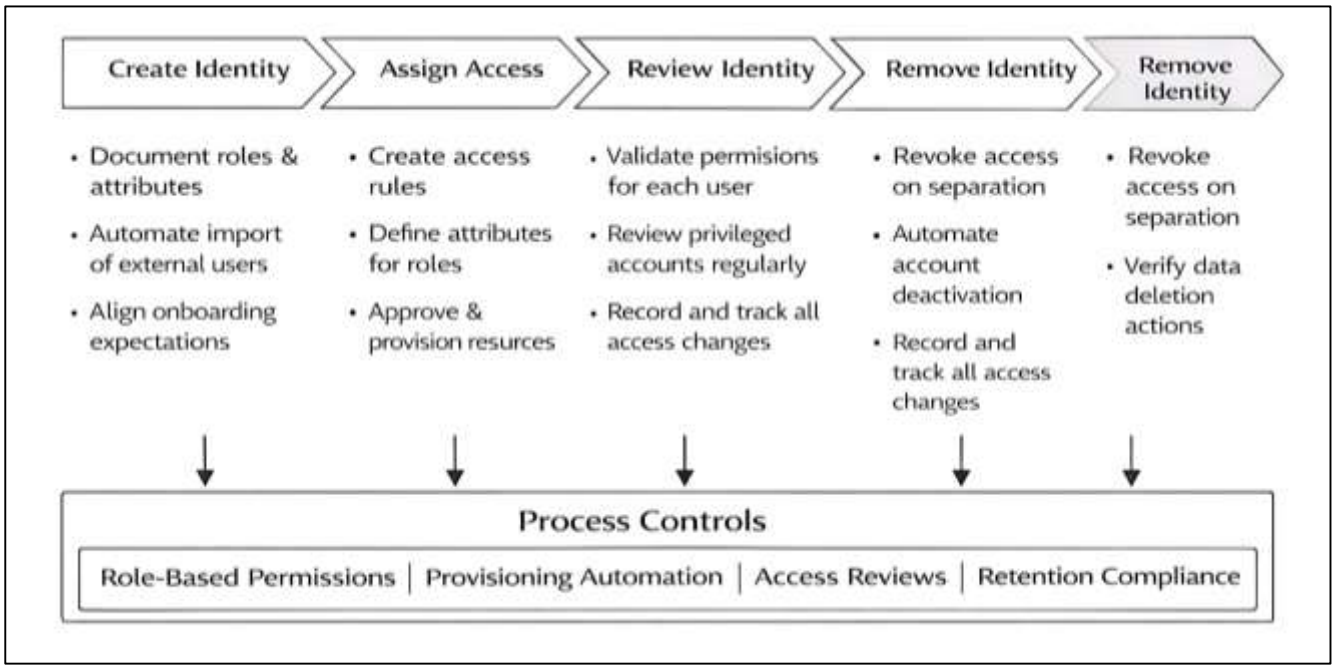
Monitoring and evidence practices constitute the third governance component because digital compliance frameworks rely on demonstrability: the ability to show that controls exist, are operating, and are producing the intended protective effects. Evidence practices include the systematic generation, retention, and review of artifacts such as access logs, configuration records, training completion records, risk assessments, incident tickets, approvals for exceptions, and vendor oversight documentation (Žigienė et al., 2019). Governance and audit literature highlights that evidence is central to assurance because accountability claims require substantiation through traceable records rather than informal assurances. In hospitality operations, evidence practices are tightly linked to platform behavior because customer data protection depends on the traceability of access, changes, and transactions across systems that support reservations, payments, loyalty programs, and guest communications. Monitoring practices enable organizations to detect unauthorized access, configuration drift, and procedural failures that may arise from frequent system updates, staff turnover, or vendor integrations. Evidence practices also extend into workforce governance, where training records and acknowledgments demonstrate that employees have been informed of their responsibilities, and into vendor governance, where assessments and attestations document third-party safeguards (S. Hu et al., 2021). From an operational perspective, evidence availability is influenced by the degree of tool centralization and integration across platforms, as fragmented systems can generate incomplete or inconsistent records that undermine verification. Quantitatively, monitoring and evidence practices can be represented through indicators capturing the completeness, accessibility, and consistency of records across properties and platforms. These indicators reflect whether the governance system supports timely audits, defensible incident investigations, and disciplined oversight of access and data handling activities. In hospitality environments characterized by distributed operations and continuous platform change, evidence practices therefore represent a measurable governance capability that underpins both internal control assurance and external accountability (Chen et al., 2020).

Process Execution Layer

Identity and access lifecycle management is a central process-execution mechanism in digital compliance frameworks because service and hospitality operations rely on large, rotating workforces and time-sensitive workflows that require rapid system access while maintaining tight control over customer data exposure (López-Pintado et al., 2019). In hospitality environments, operational platforms such as property management systems, point-of-sale systems, reservation tools, customer engagement applications, and payment environments are accessed by employees with different job roles, shift schedules, and responsibility levels. Process-oriented security and governance research emphasizes that access control effectiveness is shaped not only by the technical configuration of authentication and authorization but also by the operational discipline with which access is granted, reviewed, and removed when roles change or employment ends. Hospitality labor research repeatedly identifies high turnover and frequent staffing transitions as structural characteristics of the sector, which creates

recurring pressure on onboarding and offboarding processes and increases the risk of orphaned accounts, excessive privileges, and shared credentials. The access lifecycle can be represented as an operational chain that begins with identity creation and role assignment, moves through access provisioning aligned to job tasks, includes periodic reviews to confirm that permissions remain appropriate, and ends with timely access removal when a worker leaves or changes roles (Bera et al., 2020). Studies in information security behavior and compliance show that weak identity processes often lead to workarounds and informal access sharing, particularly in time-pressured service contexts, which can erode accountability and complicate incident investigations. Research on governance and internal controls further indicates that role-based access approaches can reduce exposure when roles are well-defined and mapped to platform permissions, allowing the organization to demonstrate consistent alignment between job responsibilities and system access. Privileged access controls receive particular attention in security and auditing literature because administrative rights and elevated permissions can be exploited to extract, alter, or delete customer data, making approvals and periodic reviews a critical process discipline. In quantitative terms, identity and access lifecycle execution can be represented through observable measures such as how quickly new staff gain appropriate access after hiring, how quickly access is removed after separation, and how regularly privileged access is reviewed and validated (Wan et al., 2022). These measurable indicators align with the literature's emphasis on operational timeliness and review discipline as necessary conditions for protecting customer data in environments characterized by distributed properties, shift-based labor, and multi-platform technology ecosystems.

Figure 6: Process Execution Framework for Compliance



Training, awareness, and workforce compliance represent a second process-execution domain because digital compliance frameworks depend on consistent employee behavior at the points where customer data is collected, accessed, and communicated. The hospitality sector's reliance on high-volume frontline service work makes behavioral adherence especially salient because staff frequently handle identity documents, payment transactions, guest communications, and preference information under time pressure (Howard & Gugger, 2020). Information security compliance research highlights that policy adherence is influenced by awareness, perceived clarity of rules, perceived consequences of non-compliance, normative expectations, and the usability of required procedures. In hospitality contexts, training effectiveness can be challenged by high turnover, seasonal hiring cycles, and varied employee backgrounds, which can create coverage gaps and inconsistent policy understanding across properties. Human resource research in hospitality emphasizes that turnover is a persistent operational feature

that increases training repetition demands, elevates the likelihood of knowledge loss, and can weaken the continuity of compliance routines across shifts and departments. Service operations research also indicates that frontline performance is shaped by routinization and standard operating procedures, suggesting that compliance training must be integrated into operational training rather than delivered as an isolated administrative requirement. Training and awareness practices are also linked to broader organizational behavior findings that employees are more likely to comply when leadership communicates the importance of policies, when rules are framed as enabling safe service delivery, and when employees perceive that compliance expectations are consistently enforced (Turetken et al., 2020). Quantitatively, workforce compliance can be represented through training completion and recertification coverage, assessments of policy knowledge or comprehension, and workforce stability indicators that capture the degree to which properties must repeatedly onboard new staff into compliance requirements. Complementary behavioral indicators can include rates of policy violations, frequency of procedural exceptions, and observed adherence to secure handling practices in daily workflows. In hospitality platform environments, training content must also cover practical platform behaviors, such as secure login practices, appropriate use of guest communication tools, secure handling of receipts and IDs, and correct escalation when suspicious activity is detected. The literature supports treating training and awareness as measurable process execution drivers that mediate the relationship between governance policies and actual control performance (Whaiduzzaman et al., 2021). When training is consistent and comprehension is high, compliance routines are more likely to be executed correctly across distributed teams; when training coverage is uneven, control execution becomes variable across properties and shifts, increasing exposure to customer data mishandling and weakening the reliability of evidence needed for audits and investigations.

Incident handling and operational response readiness form a third process-execution domain because compliance frameworks must include repeatable response routines that limit harm when customer data is threatened and demonstrate organizational accountability. Security management and incident response research emphasizes that incidents are not only technical events but organizational events that require detection, triage, communication, containment, documentation, and post-incident correction (Alaneme George & Mbadike Elvis, 2019). In hospitality and service operations, incident readiness is complicated by distributed properties, multiple operational platforms, and third-party service providers, which can fragment visibility and delay coordinated action. Service operations environments also face practical barriers to rapid reporting because frontline staff may lack technical expertise, may hesitate to report issues perceived as minor, or may prioritize guest service demands over escalation. Behavioral security research indicates that reporting behavior is shaped by clarity of procedures, psychological safety, perceived responsiveness of leadership, and whether employees believe reporting leads to constructive outcomes rather than blame. Operational readiness also depends on triage capability, which includes having defined incident categories, contact trees, escalation thresholds, and access to logs and system data needed for investigation. Containment speed is a practical performance indicator in the literature because delays can increase the likelihood of data exposure, lateral movement within networks, and broader disruption to operations. In hospitality, containment often involves actions such as disabling compromised accounts, isolating affected systems, working with vendors to restrict access, and communicating with property teams to adjust operational procedures temporarily (Xu et al., 2021). Quantitative representation of incident readiness can include how quickly an organization detects suspicious activity, how quickly it contains incidents after detection, and how consistently incidents are escalated according to documented procedures. Evidence discipline is also central, as incident response must generate records that support internal learning, compliance reporting duties, and external audit requirements. The literature supports the view that organizations with more disciplined incident processes exhibit better control over event progression and stronger accountability, while organizations with fragmented response procedures experience longer delays and weaker documentation. In multi-platform hospitality environments, response readiness therefore functions as a measurable process capability that links technical monitoring to governance obligations through structured human and organizational action under operational constraints (Maheswari et al., 2020).

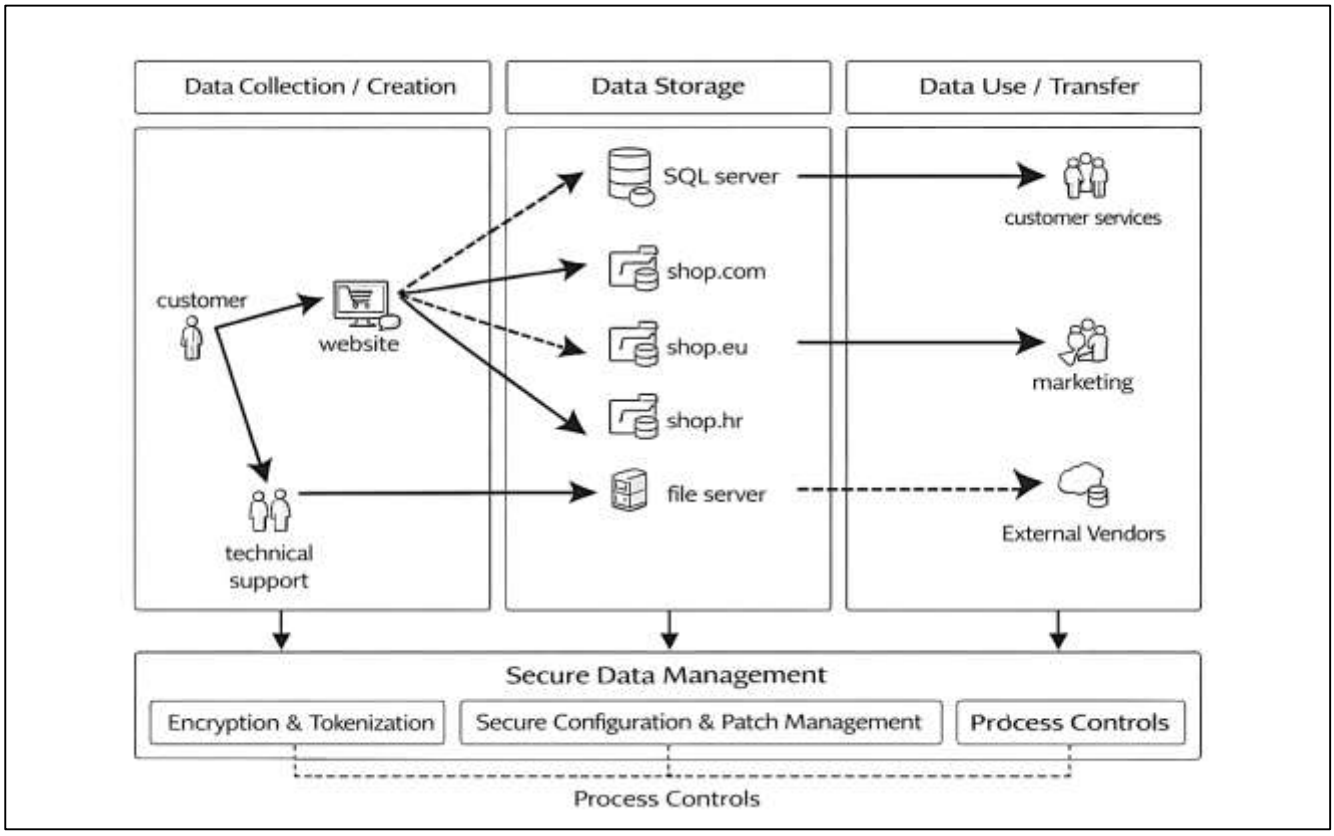
Retention and deletion workflow execution represent a fourth process-execution domain because customer data protection depends not only on preventing unauthorized access but also on controlling how long data remains stored and whether it can be reliably removed when no longer needed (Cui et al., 2020). Information governance research emphasizes that retention discipline reduces exposure by limiting the accumulation of sensitive data across operational platforms, backups, archives, and replicated environments. Privacy governance scholarship similarly highlights that retention and deletion requirements must be translated into operational workflows supported by data inventories, system configuration rules, and documented procedures for deletion requests. Hospitality operations complicate retention governance because customer data is distributed across multiple systems with different storage architectures, including on-premise property systems, cloud-managed platforms, third-party booking channels, loyalty databases, and payment-related environments. Deletion execution is often challenging because the data may be present in multiple locations, including logs, cached records, backups, and vendor-managed repositories, each requiring controlled handling to maintain integrity and compliance (Manley et al., 2021). Operational research on complex information environments supports treating retention and deletion as workflow processes rather than one-time actions, because the organization must repeatedly identify eligible data, apply retention rules, verify completion, and document actions for accountability. In hospitality contexts, retention practices also intersect with operational needs such as dispute resolution, fraud prevention, and service quality analytics, requiring clearly defined retention categories and authorization rules for exceptions. Quantitatively, retention and deletion execution can be represented through indicators of adherence to retention rules across platforms, timeliness in processing deletion requests, and reliability of backup handling practices that ensure data is not unintentionally preserved beyond permitted periods. Documentation is integral because retention actions must be auditable and traceable, particularly when data spans internal and vendor-managed systems. The literature indicates that weak retention practices increase exposure by expanding the amount of sensitive data available for compromise and by creating uncertainty about where data resides. By contrast, disciplined retention and deletion workflows strengthen compliance by limiting data footprint and supporting defensible governance (Pan et al., 2020). In service and hospitality operations platforms, retention and deletion process execution therefore function as a measurable dimension of compliance maturity that reflects how effectively governance rules are translated into repeatable operational actions across interconnected systems and distributed properties.

Technical Controls Layer Across Platforms

Encryption and data protection coverage represent a core technical-control domain in digital compliance frameworks because confidentiality risks in service and hospitality operations platforms arise from frequent data movement across networks, storage in distributed repositories, and dependence on third-party services for bookings, payments, and guest engagement (Casado-Vara et al., 2019). Security engineering literature frames encryption as a foundational safeguard that reduces the usability of data if systems are breached or communications are intercepted, while emphasizing that effective encryption depends on correct implementation, key management, and alignment with operational workflows. In hospitality environments, customer data commonly travels across reservation engines, property management systems, point-of-sale platforms, payment gateways, loyalty databases, and mobile applications, creating multiple points where data can be exposed in transit if communications are not protected. In parallel, data at rest may be stored in on-premise property servers, cloud-hosted applications, vendor-managed repositories, and analytics environments, making storage protection a multi-system requirement rather than a single-system feature (Wan et al., 2022). Payment-oriented research and compliance guidance emphasize tokenization as a specialized protection method in which sensitive payment-related data is replaced with non-sensitive tokens, limiting exposure across operational systems and reducing the number of environments where high-risk payment information must be handled. In hospitality operations, tokenization is particularly relevant because point-of-sale environments and reservation systems often interface with multiple outlets and external intermediaries, increasing the likelihood that payment signals propagate into systems not designed to store sensitive card data. The literature also highlights that encryption and tokenization operate as part of a broader confidentiality strategy that includes

access controls, secure configurations, and monitoring, because encryption does not prevent misuse by authorized users and does not remove the need for evidence and accountability. Quantitatively, encryption coverage can be represented by mapping which platforms store customer data and assessing whether stored and transmitted data is consistently protected across those platforms, while tokenization can be represented through the extent to which payment-related data is abstracted away from operational systems (Lee et al., 2020). In hospitality ecosystems where multiple properties and vendors interact, these technical protections become meaningful comparative indicators of how well a compliance framework is operationalized at the technical layer across distributed platforms and integrations.

Figure 7: Technical Data Protection Control Framework



Secure configuration management and patch or vulnerability management constitute a second technical-control domain because many security incidents arise not from the absence of security technologies but from weak configuration discipline, delayed updates, and unmanaged vulnerabilities across complex platform environments (Al Omar et al., 2019). Baseline configuration adherence refers to the extent to which systems follow defined secure settings for authentication, access control, network exposure, logging, and service hardening, reducing the likelihood of exploitation through default credentials, unnecessary services, and overly permissive settings. Risk and control literature emphasizes that configuration drift is common in operational environments where platforms are frequently updated, integrated, or modified to support new service features, and hospitality technology ecosystems exhibit these characteristics due to continuous changes in booking channels, payment integrations, and guest experience tools. Patch management research also highlights that attacker often exploit known vulnerabilities for which fixes exist, making timeliness in applying updates a crucial protection factor. Hospitality operations can struggle with update discipline because properties may operate across multiple time zones, have limited on-site IT resources, and rely on vendors for system maintenance, creating variation in how quickly security updates are applied and how consistently systems remain aligned with secure baselines (Hang & Kim, 2019). Vulnerability management includes not only applying patches but also scanning systems for weaknesses, prioritizing remediation based on severity and exposure, and documenting closure for auditability. In service and hospitality settings,

patch and configuration discipline must be balanced with operational continuity, as downtime in property management, point-of-sale, or reservation systems directly affects revenue and guest satisfaction. The literature on information security governance emphasizes that secure configuration and patching are not merely technical tasks but managed processes that require standards, accountability, and monitoring to prevent local deviations across properties. Quantitatively, configuration discipline can be represented through the proportion of platforms aligned with secure baselines and the frequency with which deviations are identified and corrected, while patch discipline can be represented through measures capturing how quickly updates are applied and how many high-risk vulnerabilities remain unresolved across platforms (Wang et al., 2019). These technical measures align with compliance expectations because they can be audited, provide evidence of due diligence, and reflect a practical capacity to maintain protective controls across an evolving platform ecosystem.

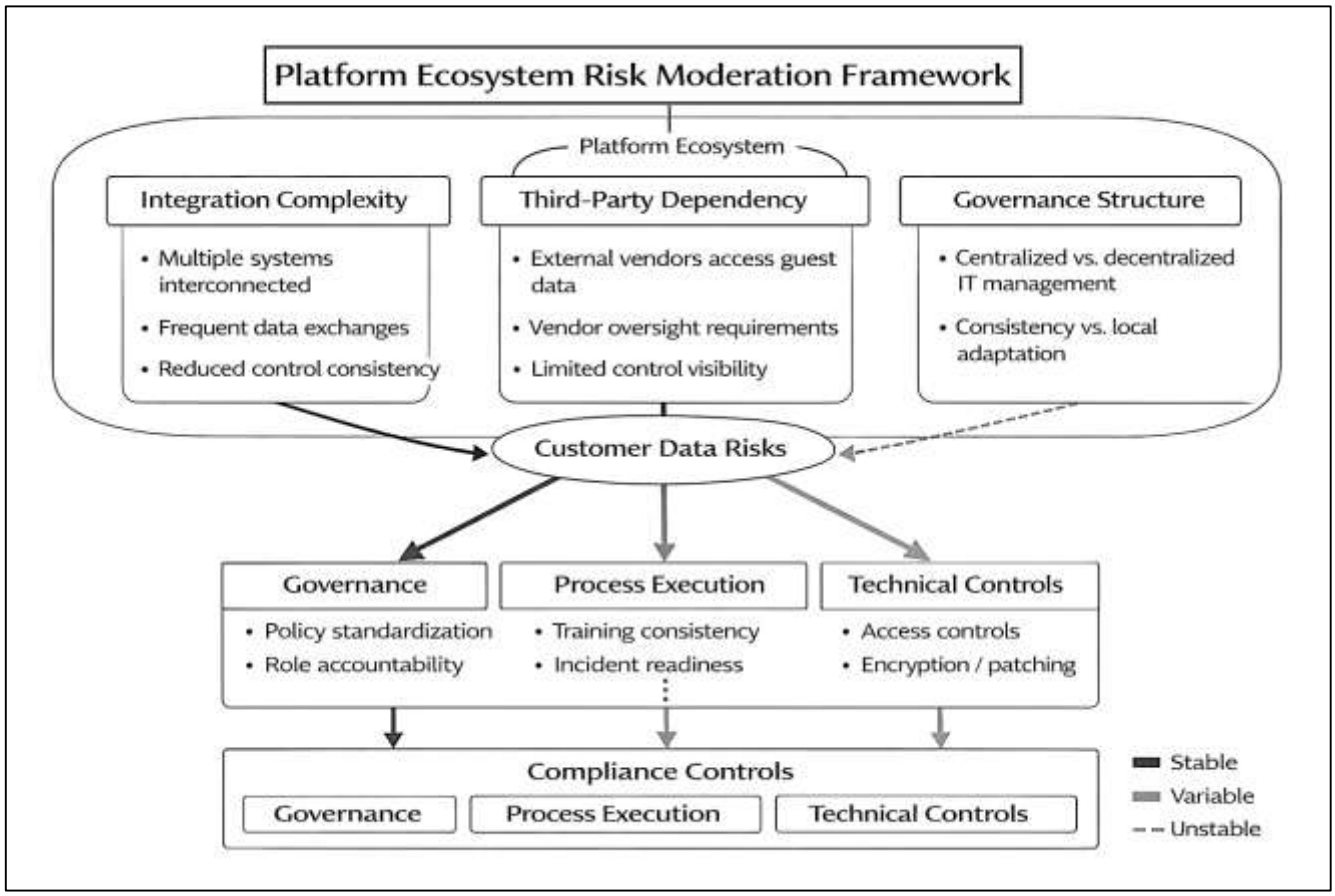
Platform Ecosystem Complexity and Third-Party Risk

Platform ecosystem complexity is repeatedly emphasized in hospitality and service technology research as a structural condition that shapes both exposure to customer data risk and the operational feasibility of maintaining consistent compliance controls across platforms. Integration complexity arises when customer data is exchanged among multiple operational systems such as reservation and distribution tools, property management systems, point-of-sale platforms, customer relationship systems, loyalty databases, guest messaging applications, Wi-Fi onboarding portals, and analytics services (Hein et al., 2020). Tourism and hospitality information systems literature describes the sector's digitization trajectory as increasingly ecosystem-based, where value creation depends on interoperability and data flows that connect internal systems to external intermediaries and service providers. Security and risk research frames each integration as a potential pathway for unintended data disclosure, misconfiguration, authentication weaknesses, or inconsistent authorization enforcement, especially when interfaces are built quickly to support operational requirements. Integration complexity also introduces governance difficulty because control responsibility becomes distributed across platform owners and vendors, while evidence for compliance must be collected from multiple systems with different logging formats and retention settings. Organizational control research suggests that as systems become more interdependent, the likelihood of control gaps increases because accountability boundaries become blurred and it becomes harder to maintain consistent baselines across all connected environments (Alt, 2021). In hospitality operations, where properties may be geographically dispersed and operate under varying local constraints, integration complexity also increases variance in configuration and operational discipline, which can lead to uneven control performance across locations even when brand-level governance is standardized. From a quantitative standpoint, integration complexity can be represented as the extent to which multiple systems are interconnected and exchange customer data routinely, capturing the operational reality that customer data protection must function across a network rather than within a single application. This view aligns with risk management scholarship emphasizing that complex interdependencies increase uncertainty and complicate assurance activities, because changes in one platform can cascade into new exposure points across the ecosystem (Aulkemeier et al., 2019). The literature therefore supports treating platform ecosystem complexity as a contextual factor that shapes how governance, process execution, and technical controls translate into measurable protection outcomes across hospitality operations platforms.

Third-party dependency functions as a risk amplifier in the literature because hospitality organizations frequently rely on external entities to perform core operational functions that directly involve customer data processing. Distribution channels, online travel agencies, booking engines, channel managers, payment processors, cloud hosting providers, identity verification services, marketing automation tools, customer support platforms, and analytics providers all represent third-party actors that may access, store, or derive insights from customer data (Floetgen et al., 2021). Studies on outsourcing and interorganizational governance emphasize that third-party dependency alters the risk profile of an organization because data protection becomes partially contingent on the vendor's controls, operational discipline, and incident response readiness. Privacy governance scholarship also stresses that compliance obligations remain attached to the organization even when processing is outsourced, requiring mechanisms for oversight, documentation, and accountability across vendor relationships.

In hospitality, third-party dependency is intensified by platform ecosystems that are assembled from modular services rather than built as a single integrated stack, making vendor exposure a routine operational condition rather than an exceptional case. Risk and threat research notes that external relationships can increase attack surface because adversaries may target weaker vendors or exploit integration pathways to access higher-value systems (Gamidullaeva et al., 2021). Vendor dependency also creates measurement challenges because evidence of control performance may be limited to vendor-provided reports, contractual attestations, or periodic assessments rather than continuous internal telemetry. Governance literature describes this as an assurance asymmetry problem, where the organization is accountable for outcomes but lacks full visibility into vendor operations. Operationally, this dependence can also influence incident handling because vendor involvement may be required to investigate logs, disable access, or remediate vulnerabilities, affecting the speed and completeness of response actions. Quantitatively, third-party dependency can be represented through the breadth of vendor relationships that touch customer data and the depth of data types shared with those vendors, reflecting the level of exposure introduced by external processing. This representation is consistent with supply-chain risk scholarship that treats vendor exposure as both a count and a scope phenomenon, because the risk implications differ when vendors access only low-sensitivity contact information versus high-sensitivity identity and payment-related data (Wang et al., 2020). The literature supports viewing third-party dependency as an amplifying condition that shapes the effectiveness of internal compliance controls and influences observable protection outcomes across hospitality operations platforms.

Figure 8: Platform Ecosystem Risk Moderation



Decentralization versus centralization of IT governance is highlighted across governance and hospitality operations research as a structural tension that affects control consistency, evidence quality, and the ability to enforce standardized compliance practices across properties. Centralized governance models typically emphasize corporate-level standardization of platforms, policies, security tooling, vendor selection, and audit programs, creating a more uniform control environment and enabling

consolidated monitoring and evidence collection (Xuelin et al., 2023). Decentralized models, which grant properties significant autonomy over platform configuration, local vendor choices, and operational procedures, can increase responsiveness to local needs and may support faster operational decision-making, yet governance literature emphasizes that decentralization can also increase variability in controls, leading to uneven compliance execution across sites. In hospitality, this tension is especially relevant because properties often differ in size, service offerings, and staffing capabilities, and some properties operate under franchise or management arrangements that complicate corporate authority over local systems. Information systems governance research treats decision rights and control ownership as central variables in explaining IT performance outcomes, and the same logic applies to compliance capability because effective controls require consistent ownership, monitoring, and enforcement. When governance is decentralized, evidence practices can become fragmented, as logs and training records may be stored locally, audits may be inconsistent, and incident escalation pathways may vary (Riasanow et al., 2021). When governance is centralized, properties may benefit from standardized tooling and centralized expertise, improving uniformity in technical baselines and reporting routines. However, operational research indicates that centralization must still account for local execution realities in service environments, including shift-based work and high turnover, which can affect adherence even under standardized policies. Quantitatively, governance structure can be represented through the degree to which decision-making and control management are concentrated at corporate level versus distributed at property level, capturing whether compliance implementation is likely to be uniform or variable across sites. This aligns with broader organizational governance literature suggesting that centralized control systems can reduce variance in compliance execution, while decentralized systems may increase local variation that must be managed through stronger coordination mechanisms (Hein et al., 2019). In service and hospitality operations platforms, governance structure therefore functions as a contextual attribute that helps explain differences in control maturity, audit performance, and incident response discipline across properties within the same brand ecosystem.

Synthesizing the literature on platform ecosystem complexity, third-party dependency, and governance structure, these contextual conditions shape customer data protection by influencing how compliance frameworks operate across interconnected service and hospitality platforms. Integration complexity increases the number of data pathways and operational dependencies, making it harder to maintain consistent access control, encryption coverage, monitoring visibility, and configuration discipline across all connected systems (Yrjölä et al., 2023). Third-party dependency extends the compliance perimeter beyond organizational boundaries, increasing exposure through vendor access and reducing direct visibility into control performance, while also introducing contractual and coordination requirements for assurance and incident response. The decentralization-centralization tension influences how consistently policies and controls are implemented across properties, with centralized governance supporting uniform standards and consolidated evidence collection and decentralized governance increasing local variability that can create control gaps. Organizational control and institutional compliance research support the view that these contextual factors interact with governance, process execution, and technical controls by shaping the complexity of implementation and the reliability of oversight (Cenamor, 2021). Risk management scholarship also reinforces that as complexity and dependency increase, the uncertainty surrounding control effectiveness grows, which can be observed through higher variability in audit findings, slower remediation, or inconsistent evidence availability across properties. Hospitality information systems research provides sector-specific grounding for these dynamics by documenting the ecosystem nature of tourism and hospitality technology and the reliance on intermediaries and service providers that process customer data. A quantitative framing consistent with this literature treats these contextual factors as measurable characteristics of the operational environment that explain why the same compliance framework maturity may yield different protection outcomes across organizations or properties (Pauli et al., 2021). By embedding platform complexity, vendor dependency, and governance structure into the literature review as contextual drivers, the study's conceptual model gains operational realism and supports empirical analysis of how compliance frameworks perform under varying ecosystem conditions in service and hospitality operations platforms.

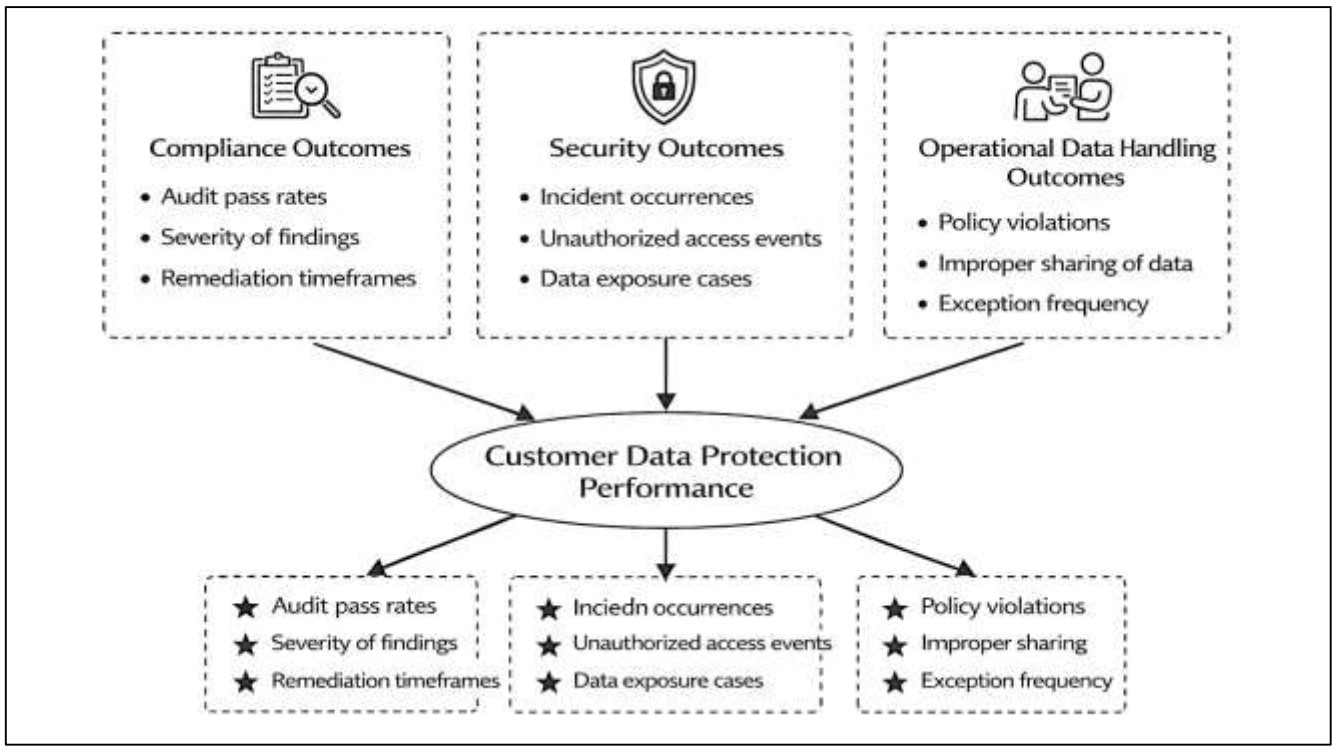
Customer Data Protection Performance

Customer data protection performance in service and hospitality operations can be treated as an outcomes domain that captures how well an organization converts governance, process execution, and technical controls into observable compliance and security results across operational platforms that store, process, and transmit customer information (Taufick, 2021). The literature on information security governance emphasizes that performance should be evidenced through verifiable indicators rather than inferred from the mere presence of policies or technologies, because organizations often exhibit a gap between formal compliance structures and day-to-day control operation. In hospitality contexts, where the operational environment is distributed and platform ecosystems are interconnected, performance measurement becomes especially important because customer data flows across reservation systems, property management systems, point-of-sale environments, customer relationship management tools, loyalty systems, and third-party services. Compliance scholarship frequently frames performance in terms of assurance and verification outcomes, where audits function as structured evaluations of whether controls are appropriately designed, implemented, and operating consistently. Audit-based outcomes can be described through three complementary dimensions: the proportion of audits or assessments that meet predefined requirements without major deficiencies, the seriousness of findings identified during assessments, and the time required to close gaps through remediation (Martin et al., 2019). These dimensions reflect not only technical weaknesses but also organizational discipline, because recurring findings and slow remediation often indicate systemic issues in ownership, prioritization, and monitoring. The audit and verification literature also suggests that severity-weighted evaluation is more informative than simple counts because the impact of a small number of critical failures can exceed the risk posed by numerous minor documentation gaps. In hospitality operations, audit performance is also shaped by the sector's reliance on payment processing and third-party platforms, which increases the number of control domains subject to scrutiny and expands evidence requirements. A quantitative view that defines compliance performance through audit results and remediation discipline aligns with the literature's emphasis on accountability and demonstrability, capturing whether the organization can consistently show control operation across properties and platforms (Okazaki et al., 2020). This approach also supports comparative analysis because audit outcomes can be aggregated at the property level, brand level, or platform level to represent compliance performance in ways that are consistent across diverse hospitality business models.

Security outcomes form a second outcomes domain because compliance frameworks ultimately aim to reduce unauthorized access, prevent data exposure, and limit the frequency and severity of incidents affecting customer data. Security performance is commonly represented in the literature through observable events such as the occurrence of incidents, the rate of unauthorized access attempts or confirmed unauthorized accesses, and the incidence of data exposure cases that involve customer information (Fernando et al., 2023). Research on breaches and cyber risk indicates that incidents are not homogeneous; they vary in cause, scale, and operational consequences, but they share a common relevance for performance measurement because they indicate a breakdown or bypassing of protective controls. In hospitality, security outcomes are closely tied to platform characteristics and operational realities: distributed properties may have uneven configuration discipline, staff turnover may increase credential-related risk, and third-party integrations may create exposure pathways that are difficult to monitor. Security economics and risk management scholarship emphasizes that organizations manage security under uncertainty, making event-based indicators valuable because they provide concrete evidence of realized risk rather than theoretical vulnerability. The incident response literature also highlights that organizational capacity to detect and contain incidents affects how security events translate into harm, meaning that frequency measures can be complemented by measures capturing the occurrence of exposure cases and unauthorized access events. In practical hospitality operations, unauthorized access may include misuse of employee credentials, exploitation of misconfigured system interfaces, or vendor-related access failures, while exposure cases may involve accidental disclosure through messaging tools, unsecured file transfers, or compromised endpoints in property networks (Keszey, 2020). Measurement research in security governance supports counting security incidents and access violations as outcome indicators because they provide empirical anchors for

testing whether higher compliance maturity and stronger control execution correspond to fewer adverse events. At the same time, the literature recognizes that measurement quality depends on consistent logging and reporting practices, as organizations with stronger monitoring may detect more events, which can complicate interpretation. Therefore, security outcomes are frequently examined in combination with governance and monitoring maturity to distinguish between true increases in risk and increases in detection visibility (Zheng et al., 2022). In hospitality ecosystems, this combined approach is particularly relevant because monitoring capacity can vary across properties and vendor-managed platforms, influencing both the recorded frequency of incidents and the organization's ability to document unauthorized access events credibly.

Figure 9: Customer Data Protection Performance Outcomes



Operational data handling outcomes represent a third outcomes domain that connects customer data protection to everyday human and procedural behaviors that occur during service delivery. The literature on information security compliance and organizational behavior indicates that policy adherence is a crucial determinant of protection performance because many data exposures occur through routine actions such as improper sharing, unauthorized disclosure, careless handling of identity documents, weak credential practices, or bypassing secure procedures to save time in high-pressure environments (Chouaibi et al., 2022). Hospitality operations are particularly sensitive to these issues because service encounters occur in public-facing settings where employees must act quickly, communicate across departments, and use multiple systems to resolve customer needs. Operational data handling outcomes can therefore be represented through observable indicators such as the frequency of policy violations, improper data sharing events, and exception rates where staff or properties deviate from standard procedures. These outcomes reflect the practical effectiveness of compliance training, role clarity, and process execution, providing a human-centered performance perspective that complements audit and incident metrics. Behavioral security research supports measuring policy violations because it links compliance outcomes to deterrence perceptions, normative influences, perceived behavioral control, and clarity of expectations, all of which can vary significantly across hospitality properties and workforce segments. From an operational control standpoint, exception rates also provide insight because frequent exceptions may indicate misalignment between policy design and operational feasibility, suggesting that controls are not well integrated into workflows (Shin, 2019). Operational data handling outcomes may also capture communication-related

exposures, such as sharing customer details through unsecured channels, discussing sensitive information in inappropriate contexts, or retaining copies of documents beyond permitted periods. In platform-rich hospitality settings, policy violations can occur within systems as well, such as accessing customer records without business need, exporting data without authorization, or failing to follow required steps for verifying identity during account changes. These outcomes provide a granular view of performance because they reveal whether customer data protection is embedded into routine work behavior across service touchpoints rather than expressed only in formal governance structures (Shin, 2019). When examined quantitatively, these indicators allow researchers to test whether stronger compliance frameworks correspond to lower rates of operational violations and fewer exceptions across properties and platforms.

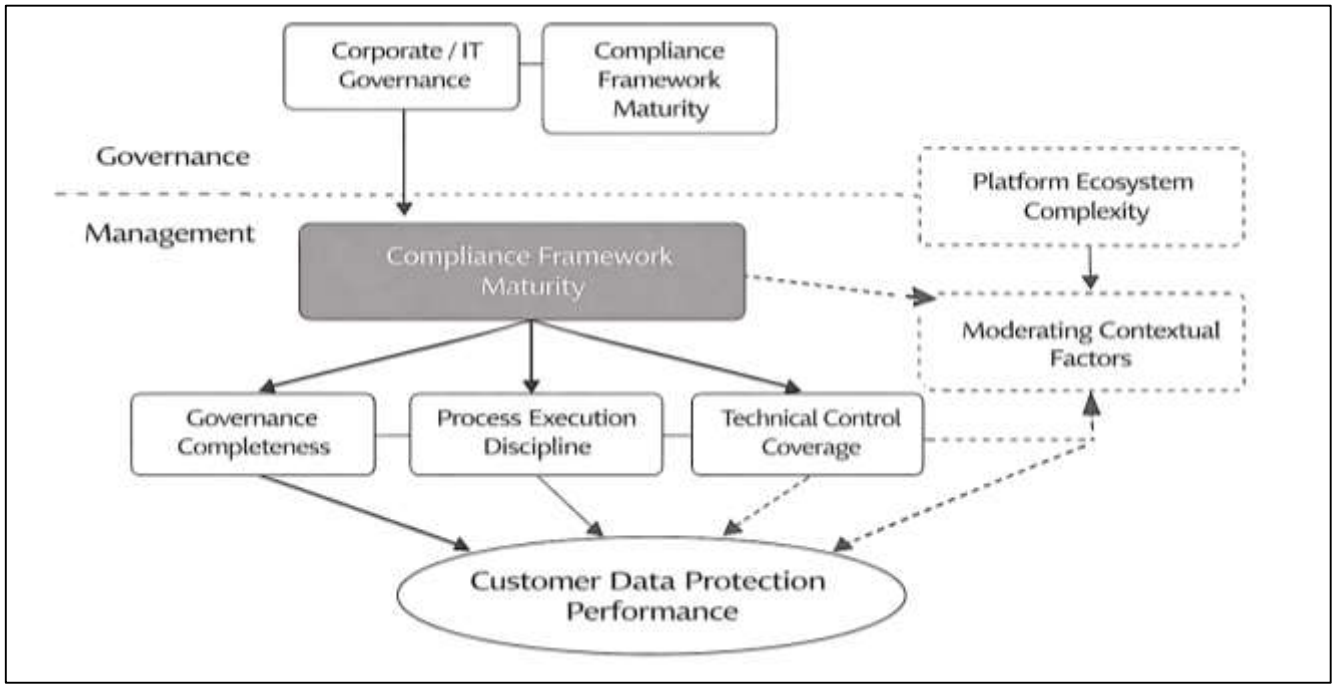
Synthesizing compliance outcomes, security outcomes, and operational data handling outcomes, the literature supports treating customer data protection performance as a multidimensional construct that reflects both verification-based measures and event-based measures. Audit pass rates, severity profiles of findings, and remediation discipline represent structured assurance outcomes that capture whether controls are operating and improving over time under formal assessment (Li et al., 2023). Incident occurrence, unauthorized access events, and data exposure cases represent realized security outcomes that indicate whether controls are successfully preventing harmful events in the operational environment. Policy violations, improper sharing, and exception frequency represent behavioral and procedural outcomes that reveal the extent to which compliance requirements are enacted during everyday service delivery. This multidimensional approach is consistent with governance and risk management scholarship that emphasizes the need to triangulate performance using both compliance assurance indicators and operational event indicators, because any single measure can be incomplete. For example, strong audit results may coexist with unreported operational violations if monitoring and reporting are weak, while higher recorded incident counts may reflect improved detection rather than worsening security (Hanif & Lallie, 2021). Therefore, the literature supports using multiple outcome domains to capture protection performance in a balanced manner that reflects verification, security events, and human process adherence. In hospitality and service operations platforms, where customer data is processed across interconnected systems and distributed properties, these outcome domains provide an operationally meaningful basis for evaluating protection performance across contexts. By defining the dependent variable through measurable compliance, security, and operational handling outcomes, the quantitative model can examine how governance, process execution, technical controls, and ecosystem complexity relate to customer data protection performance across hospitality operations platforms (Prybutok & Sauser, 2022).

Model Development from Literature

Quantitative model development for digital compliance frameworks in service and hospitality draws on governance, security management, privacy governance, and service operations literatures that emphasize measurable relationships between organizational controls and observable protection outcomes (Ramírez-Montoya et al., 2022). A core synthesis across these streams is that compliance capability is not adequately represented by single policies or isolated technologies, because protection performance emerges from a coordinated system that combines governance structures, operational process discipline, and technical safeguards across multiple platforms that handle customer data. Information systems governance research highlights that organizations achieve stronger control performance when decision rights and accountability are clearly assigned and consistently enforced across units, which supports modeling compliance maturity as a latent capability reflected by governance completeness, process execution discipline, and technical control coverage (Senyo et al., 2019). Security management standards literature reinforces that measurable assurance requires control objectives that are mapped to operational routines and evidence repositories, making it empirically reasonable to test whether organizations with higher compliance framework maturity exhibit stronger performance on audit-based outcomes and lower rates of security incidents and operational violations. Privacy governance research similarly frames accountability as demonstrability and repeatability, implying that mature compliance systems should be associated with more favorable verification outcomes and more disciplined remediation cycles. Service and hospitality platform scholarship contributes sector specificity by showing that customer data is processed across interdependent

systems, meaning outcomes are shaped by system interoperability and the degree to which controls remain consistent across platforms and properties. A quantitative synthesis therefore proposes a direct relationship between overall compliance framework maturity and customer data protection performance measured through compliance assurance results, security event occurrence, and operational handling discipline (Mengist et al., 2020). This synthesis is consistent with risk management and security economics work that treats organizational capability as a determinant of realized risk and loss, and with auditing scholarship that frames assessment outcomes as indicators of control quality. The model foundation also accommodates institutional perspectives that organizations under stronger regulatory and stakeholder scrutiny formalize governance, implement standardized controls, and expand monitoring evidence, creating measurable variation in maturity and performance across hospitality organizations. In this way, the core model proposition is grounded in multiple literatures that converge on the idea that a higher maturity compliance framework corresponds to stronger customer data protection performance, while recognizing that the hospitality context introduces complexity through distributed properties, high workforce turnover, and multi-vendor platform ecosystems (Kumar et al., 2023).

Figure 10: Quantitative Compliance Framework Model



A second synthesis theme is that the strength of the relationship between compliance framework maturity and outcomes is conditioned by platform ecosystem complexity and third-party dependency, which are widely treated in the literature as contextual factors that amplify exposure and complicate control execution (Golan et al., 2020). Hospitality information systems research describes the sector's technology environment as ecosystem-based, where value creation relies on integrations among internal systems and external intermediaries, making customer data protection dependent on interface security, consistent authorization, and coordinated evidence collection across multiple applications. Security and threat research emphasizes that each integration introduces new pathways for misconfiguration and exploitation, while outsourcing and supply-chain risk research highlights that vendor access expands attack surface and reduces direct organizational visibility into control performance. These insights support modeling integration complexity and vendor data access breadth as contextual conditions that influence how effectively a compliance framework translates into outcomes. In empirical terms, the same maturity level can yield different outcomes depending on how many systems exchange customer data and how many external entities touch sensitive information (Snyder, 2019). Governance literature further suggests that complexity increases coordination demands and raises the probability of control gaps, because responsibility becomes distributed across platform

owners and vendors with differing priorities and evidence practices. Incident response research also implies that third-party dependency affects operational readiness by adding coordination steps to investigations and remediation, which can influence detection and containment performance and increase the likelihood that operational violations persist longer. The quantitative synthesis therefore treats ecosystem complexity and vendor exposure as moderators that shape the magnitude and consistency of observed relationships between compliance maturity and outcomes. In hospitality settings, where properties may rely on vendor-managed platforms for core functions such as booking, payments, and guest engagement, third-party dependency also interacts with governance and monitoring capacity, influencing both the occurrence of security incidents and the organization's ability to document and remediate issues (Carrera-Rivera et al., 2022). This synthesis aligns with the broader measurement perspective that performance outcomes should be interpreted within the operational environment in which controls operate, and it supports an empirically testable model where ecosystem complexity and vendor dependency help explain why outcomes vary across organizations with similar governance intentions (Han et al., 2020).

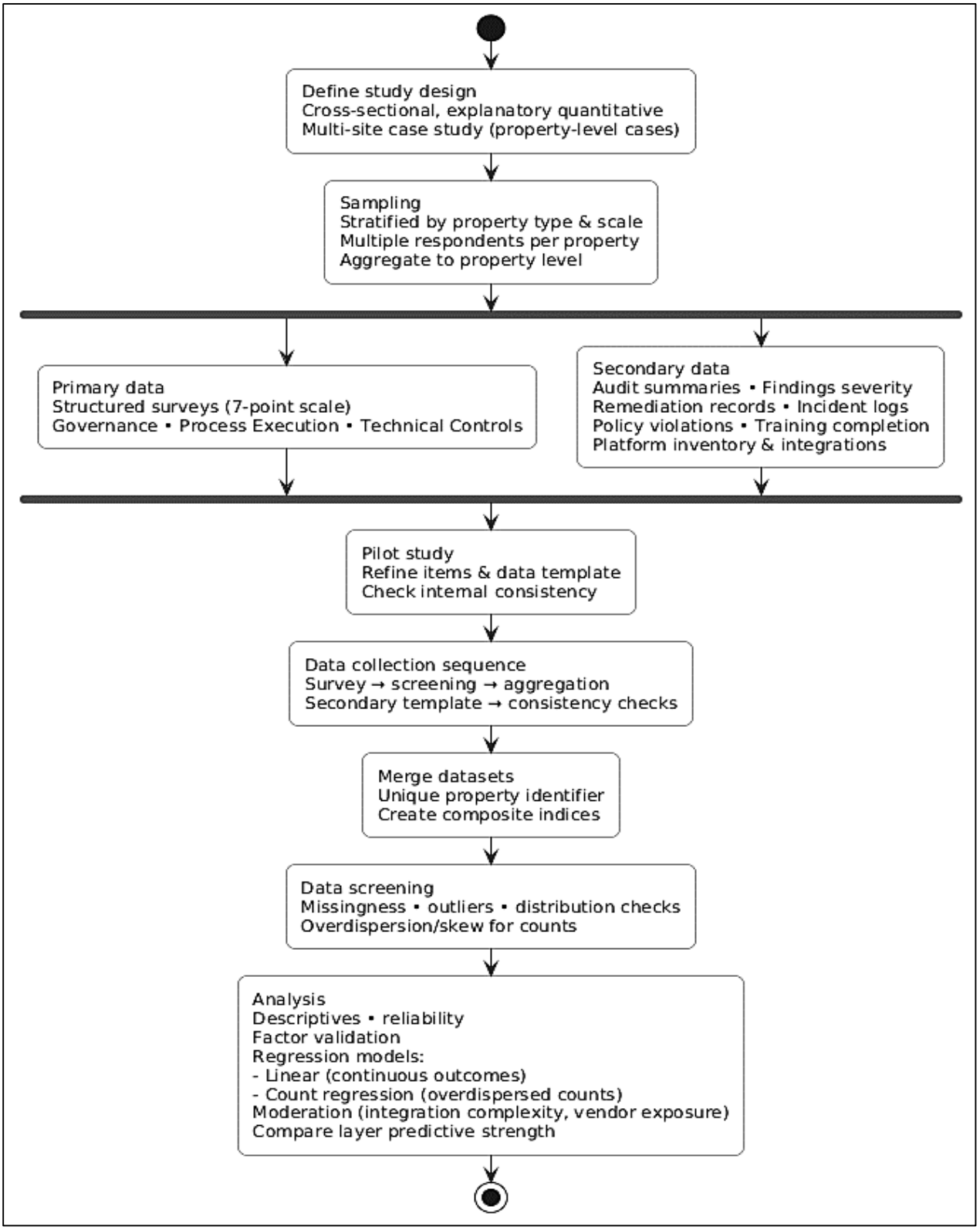
METHOD

A cross-sectional, explanatory quantitative research design was applied to examine how digital compliance frameworks were associated with customer data protection performance across service and hospitality operations platforms. The study was structured as a multi-site case study because data were compiled from multiple operational units that shared comparable platform categories but differed in ecosystem complexity, vendor dependency, and governance structure. Each case was defined as an individual service or hospitality property that operated at least three core digital platforms that processed customer data, including reservation-related systems, transaction platforms, and customer engagement or profile systems. The case study description therefore captured the operational setting in which customer data moved across front-of-house and back-of-house processes, and it documented key contextual attributes such as the platform footprint, the degree of system interoperability, and the extent of third-party involvement in processing customer information. The population comprised service and hospitality properties that used digitally integrated operations platforms and processed customer data as part of routine service delivery. A stratified sampling technique was used to ensure representation across property types and operational scale, including hotels, resorts, and restaurant or multi-outlet service sites, and the sample was drawn to include small, medium, and large properties so that the results reflected variation in exposure and resource capacity. The final sample included multiple respondents per property to reduce single-source bias, and responses were aggregated at the property level after consistency checks were completed. The sampling approach was implemented to support statistical comparison across properties while maintaining case-based documentation of platform configurations and governance arrangements within each participating unit.

Data were collected as both primary and secondary data to strengthen measurement validity and reduce reliance on perceptual reporting alone. Primary data were gathered using structured surveys that captured governance layer implementation, process execution discipline, technical control coverage perceptions, and IT governance structure characteristics. Secondary data were extracted from property records and organizational documentation, including audit summaries, severity classifications of findings, remediation records with closure dates, incident logs documenting security events and unauthorized access occurrences, policy violation reports, training completion records, and platform inventory documentation that described the operational systems in use and their integration relationships. Measurement scales were standardized to support quantitative modeling: perceptual survey items were measured using a seven-point agreement scale, while outcome measures were recorded using operational counts, time-based values, and severity categories aligned to established internal assessment practices. Variables were operationalized through composite indices created from multiple items within each construct, including governance quality indicators such as role clarity and policy standardization, process execution indicators such as access lifecycle discipline, training coverage, incident escalation adherence, and retention workflow execution, and technical control indicators such as encryption coverage, configuration discipline, logging completeness, and segmentation practices. A pilot study was conducted prior to full deployment to evaluate item clarity, completion time, and internal consistency of multi-item constructs, and pilot feedback was used to

refine ambiguous wording, remove redundant items, and improve alignment between survey items and the operational data fields requested for secondary extraction. The pilot also supported refinement of the data request template to ensure that audit, remediation, and incident records could be consistently compiled across properties and merged using a unique property identifier.

Figure 11: Methodology of this study



Data collection procedures were implemented in a structured sequence to support consistent integration of survey responses with operational metrics at the property level. Survey links were distributed to designated roles at each property, including operational management and technology or compliance-related personnel, and responses were screened for completeness and attention checks before aggregation. A standardized data template was then used to collect secondary metrics for a defined retrospective period, and records were reviewed for consistency in date formats, severity labeling, and duplication. Data were merged into a single analytical dataset, and screening procedures were applied to identify missing values, outliers, and distributional issues, with count-based outcomes evaluated for overdispersion and skew. Data analysis techniques included descriptive statistics, reliability assessment of multi-item constructs, factor-based validation procedures for construct structure, and multivariate hypothesis testing using regression-based models. Linear regression models were applied for continuous outcomes such as remediation duration, while count-based outcomes such as incident counts and policy violations were analyzed using count regression methods appropriate for over dispersed distributions. Moderation analysis was conducted using interaction terms to evaluate whether integration complexity and vendor exposure altered the strength of the relationships between compliance framework maturity and outcomes, and comparative modeling was conducted to evaluate whether governance, process execution, or technical control layers demonstrated different predictive strengths across outcome categories. All analyses were conducted using statistical software suitable for regression, factor analysis, and visualization, and data preparation workflows were managed using spreadsheet tools and scripting utilities to support reproducibility and consistent transformation of operational records into analysis-ready variables.

FINDINGS

Descriptive Analysis

The descriptive analysis was conducted to summarize the dataset characteristics and confirm suitability for later inferential testing. The property-level measures showed moderate-to-high central tendencies for governance quality, process execution strength, and technical control maturity, indicating that many properties maintained formal compliance practices while still exhibiting noticeable gaps. Platform ecosystem complexity and third-party dependency varied widely across the sample, which indicated that some properties operated within relatively simple platform environments while others used highly integrated systems with extensive vendor access. Outcome measures also demonstrated clear variability, as audit performance differed across properties and event-based measures such as security incidents and data-handling violations ranged from low to comparatively high values. Distributional review indicated that event-based outcomes were positively skewed, which justified later use of appropriate modeling choices for count-type outcomes. Overall, variability across constructs and controls supported multivariate testing.

Table 1: Descriptive Statistics for Compliance Framework Predictors and Contextual Factors

Variable	Mean	SD	Min	Max
Governance quality (1–7)	5.21	0.88	2.40	6.90
Process execution strength (1–7)	5.03	0.92	2.10	6.80
Technical control maturity (1–7)	4.87	0.97	2.00	6.70
Overall compliance maturity (1–7)	5.04	0.79	2.30	6.70
Platform ecosystem complexity (index)	8.60	3.10	3.00	18.00
Third-party dependency (index)	6.40	2.80	1.00	14.00
IT governance centralization (1–7)	4.62	1.13	1.60	6.90

Table 1 summarized the main predictors and contextual factors. Governance quality, process execution, and technical controls showed moderately high mean values, indicating that many properties had established compliance structures, although the standard deviations suggested meaningful dispersion in implementation strength. Overall compliance maturity also demonstrated variation, supporting the

presence of both lower- and higher-maturity environments. Platform ecosystem complexity and third-party dependency exhibited broad ranges, reflecting substantial heterogeneity in integration burden and vendor exposure. IT governance centralization ranged from low to high, showing that properties differed in the extent to which decision rights and control ownership were coordinated through corporate structures versus local autonomy.

Table 2: Descriptive Statistics for Customer Data Protection Outcomes and Control Variables

Variable	Mean	SD	Min	Max
Audit pass performance (0–100)	82.30	9.60	55.00	98.00
Severity of audit findings (score)	12.40	7.10	0.00	35.00
Remediation cycle time (days)	38.20	21.50	7.00	120.00
Security incidents (12 months, count)	2.10	2.60	0.00	14.00
Unauthorized access events (12 months, count)	1.30	2.00	0.00	11.00
Data-handling violations (12 months, count)	3.40	3.90	0.00	20.00
Property size (employees)	142.00	96.00	25.00	520.00
Transaction volume (monthly, count)	18,500	14,200	2,100	72,000
Workforce turnover (annual, %)	41.80	16.70	12.00	88.00
Cloud adoption level (0–100)	63.50	18.90	20.00	95.00

Table 2 presented outcome indicators and control variables. Audit pass performance indicated generally favorable compliance results, yet severity scores and remediation timelines suggested persistent weaknesses that required operational follow-through. Count-based outcomes showed wide dispersion, with some properties reporting no incidents or violations and others reporting elevated event frequencies. Remediation time varied substantially, indicating differences in resource capacity and closure discipline across sites. Control variables showed large ranges in property size and transaction volume, confirming heterogeneous operational exposure. Workforce turnover was high on average and varied widely, supporting its relevance as a contextual control for access governance and training stability.

Correlation

Correlation analysis was conducted to evaluate bivariate associations among the compliance framework dimensions, contextual factors, outcomes, and key controls prior to multivariate modeling. The results showed that governance quality, process execution discipline, and technical control maturity were strongly interrelated yet remained below redundancy thresholds, indicating that the constructs represented related but distinct compliance dimensions. Each maturity dimension was positively associated with compliance performance, reflected by higher audit pass performance and lower severity of audit findings and shorter remediation duration. In contrast, higher maturity was negatively associated with security incidents, unauthorized access events, and operational data-handling violations, which indicated that stronger compliance capability aligned with better protection outcomes. Contextual factors displayed the expected risk pattern: platform ecosystem complexity and third-party dependency were positively correlated with incident-related outcomes and violations, indicating greater exposure in highly integrated and vendor-dependent environments. Property size and transaction volume were positively associated with incidents and violations, supporting their inclusion as controls to account for operational exposure differences.

Table 3: Correlation Matrix for Compliance Maturity Dimensions, Contextual Factors, and Compliance Outcomes

Variable	1	2	3	4	5	6	7
1. Governance quality	1.00						
2. Process execution strength	0.71	1.00					
3. Technical control maturity	0.66	0.68	1.00				
4. Overall compliance maturity	0.86	0.88	0.84	1.00			
5. Platform ecosystem complexity	-0.18	-0.16	-0.22	-0.20	1.00		
6. Third-party dependency	-0.14	-0.12	-0.19	-0.16	0.58	1.00	
7. Audit pass performance	0.49	0.44	0.52	0.55	-0.21	-0.18	1.00
8. Severity of audit findings	-0.46	-0.39	-0.50	-0.53	0.24	0.20	-0.61

Table 3 reported correlations among compliance maturity dimensions, contextual factors, and compliance outcomes. Governance, process execution, and technical controls were strongly correlated with each other, but the values remained below typical redundancy thresholds, indicating that the constructs captured distinct layers of compliance. Overall compliance maturity showed a positive association with audit pass performance and a negative association with severity of audit findings, which indicated better compliance outcomes in higher-maturity properties. Platform ecosystem complexity and third-party dependency were negatively associated with audit pass performance and positively associated with audit finding severity, suggesting that integrated and vendor-dependent environments faced greater compliance burden and control variability.

Table 4: Correlation Matrix for Contextual Factors, Security and Operational Outcomes, and Key Controls

Variable	1	2	3	4	5	6	7	8
1. Platform ecosystem complexity	1.00							
2. Third-party dependency	0.58	1.00						
3. Security incidents	0.33	0.29	1.00					
4. Unauthorized access events	0.30	0.27	0.69	1.00				
5. Data-handling violations	0.28	0.31	0.55	0.49	1.00			
6. Remediation cycle time	0.22	0.19	0.26	0.21	0.24	1.00		
7. Property size	0.25	0.18	0.34	0.28	0.23	0.17	1.00	
8. Transaction volume	0.29	0.21	0.37	0.30	0.26	0.19	0.62	1.00
9. Overall compliance maturity	-0.20	-0.16	-0.36	-0.32	-0.41	-0.29	-0.08	-0.10

Table 4 summarized associations among contextual exposure factors, outcomes, and key controls. Platform ecosystem complexity and third-party dependency showed positive correlations with security incidents, unauthorized access events, and data-handling violations, indicating higher exposure in environments with heavier integration and vendor access. Incident-related outcomes were strongly correlated with each other, suggesting clustering of security issues in the same properties. Remediation cycle time was positively correlated with incidents and violations, indicating that slower closure discipline co-occurred with weaker protection outcomes. Property size and transaction volume were positively associated with incident and violation outcomes, supporting their role as exposure controls in later regression models.

Reliability and Validity

Reliability analysis was conducted to evaluate internal consistency of the multi-item constructs representing governance quality, process execution strength, technical control maturity, and overall

compliance framework maturity. The results showed that all constructs exceeded commonly accepted reliability thresholds, confirming that the measurement items were consistently aligned within each construct. Construct validity was assessed using factor-based procedures that evaluated whether measurement items loaded strongly onto their intended factors and whether the three compliance layers remained empirically distinguishable. The standardized loadings were substantial and statistically meaningful, indicating strong item representation of each construct and supporting convergent validity. Discriminant validity was supported because inter-construct correlations remained below levels indicating construct redundancy, and the variance captured by each construct exceeded the variance shared with other constructs. Collectively, these reliability and validity results indicated that the measurement model was robust and appropriate for hypothesis testing using regression-based models.

Table 5: Internal Consistency Reliability for Multi-Item Constructs

Construct	Items (k)	Cronbach's α	Composite Reliability
Governance quality	8	0.91	0.93
Process execution strength	9	0.89	0.91
Technical control maturity	10	0.90	0.92
Overall compliance maturity	27	0.95	0.96
IT governance centralization	5	0.86	0.88
Incident response readiness	6	0.88	0.90

Table 5 indicated that internal consistency reliability was strong across all constructs. Cronbach's alpha values ranged from 0.86 to 0.95, which suggested that item sets were highly coherent and measured the intended underlying dimensions reliably. Composite reliability values were similarly high, reinforcing the stability of the constructs under latent measurement assumptions and supporting their suitability for multivariate modeling. The overall compliance maturity construct demonstrated the highest consistency due to its larger item pool reflecting the combined governance, process, and technical layers. These reliability results confirmed that the instrument produced consistent measurements across properties and that scale scores were appropriate for subsequent correlation and regression testing.

Table 6: Validity Evidence: Factor Loadings and Convergent/Discriminant Validity Indicators

Construct	Loading Range	AVE	Highest Inter-Construct Correlation	√AVE
Governance quality	0.68–0.88	0.61	0.71	0.78
Process execution strength	0.64–0.86	0.58	0.71	0.76
Technical control maturity	0.66–0.89	0.60	0.68	0.77
IT governance centralization	0.62–0.84	0.55	0.42	0.74
Incident response readiness	0.65–0.87	0.59	0.49	0.77

Table 6 provided convergent and discriminant validity evidence. The standardized loading ranges indicated that individual items were strongly associated with their intended constructs, supporting convergent validity at the indicator level. Average variance extracted values were above 0.50 for all constructs, indicating that each construct captured more than half of the variance in its indicators. Discriminant validity was supported because the square root of AVE for each construct exceeded its highest correlation with any other construct, indicating that the constructs remained empirically distinct rather than overlapping excessively. These results confirmed that governance, process execution, and technical controls represented separable measurement domains suitable for hypothesis testing.

Collinearity

Collinearity diagnostics were performed to assess whether linear dependence among predictor variables could bias regression estimates or inflate standard errors. Variance inflation factor and tolerance statistics were examined for all independent variables, moderators, and control variables included in the regression models. The results demonstrated that all variance inflation factor values were well below commonly accepted critical thresholds, and tolerance values remained comfortably above minimum cut-off levels. These findings indicated that each predictor contributed distinct explanatory information to the models. Particular attention was given to governance quality, process execution strength, and technical control maturity, as these constructs were conceptually related components of compliance frameworks. The diagnostics confirmed that these dimensions were sufficiently independent to be modeled simultaneously without compromising interpretability. Control variables related to operational scale, workforce dynamics, and technology deployment also demonstrated stable collinearity properties. Overall, the diagnostics confirmed that the regression models were not adversely affected by multicollinearity and that all predictors could be retained for hypothesis testing.

Table 7: Collinearity Diagnostics for Compliance Framework Predictors and Moderators

Predictor Variable	Tolerance	VIF
Governance quality	0.48	2.08
Process execution strength	0.44	2.27
Technical control maturity	0.46	2.17
Overall compliance maturity	0.39	2.56
Platform ecosystem complexity	0.63	1.59
Third-party dependency	0.66	1.52
IT governance centralization	0.71	1.41

Table 7 reported tolerance and variance inflation factor values for the primary predictors and moderators. All tolerance values exceeded 0.39, and variance inflation factors ranged from 1.41 to 2.56, indicating low to moderate correlation among predictors without reaching problematic levels. Governance quality, process execution strength, and technical control maturity demonstrated slightly higher variance inflation factors than contextual variables, reflecting their conceptual relatedness, yet the values remained well below thresholds that indicate redundancy. Platform ecosystem complexity, third-party dependency, and IT governance centralization showed particularly low variance inflation factors, suggesting strong independence from the core compliance constructs. These results supported inclusion of all predictors in the regression models.

Table 8: Collinearity Diagnostics for Control Variables Included in Regression Models

Control Variable	Tolerance	VIF
Property size	0.58	1.72
Transaction volume	0.54	1.85
Workforce turnover rate	0.69	1.45
Geographic region	0.77	1.30
Cloud adoption level	0.62	1.61

Table 8 summarized collinearity diagnostics for control variables capturing operational scale, workforce dynamics, geographic dispersion, and technology deployment. Tolerance values ranged from 0.54 to 0.77, while variance inflation factors ranged from 1.30 to 1.85, indicating minimal shared variance among controls. Property size and transaction volume showed moderate association, as

expected in service operations, yet their variance inflation factors remained well within acceptable bounds. Workforce turnover, geographic region, and cloud adoption demonstrated strong independence from other controls. These diagnostics confirmed that inclusion of control variables did not introduce instability into the regression models and allowed for reliable adjustment of contextual effects.

Regression and Hypothesis Testing

Hierarchical regression analysis was conducted to evaluate the predictive effect of compliance framework maturity on customer data protection performance across service and hospitality operations platforms while adjusting for operational exposure and technology context. The results showed that compliance framework maturity was a significant predictor of improved compliance outcomes, including higher audit pass performance and lower audit finding severity. Compliance maturity was also significantly associated with reduced adverse outcomes, including fewer security incidents and fewer operational data handling violations, indicating stronger protection capability in higher-maturity properties. The moderation results indicated that platform ecosystem complexity and third-party dependency altered these associations, as the impact of compliance maturity on protection outcomes strengthened in more complex and vendor-exposed environments. Comparative layer models further showed differentiated predictive patterns: governance quality was more strongly associated with audit-related outcomes, technical control maturity exhibited stronger relationships with incident outcomes, and process execution strength showed stronger relationships with operational handling outcomes. Model fit indices and explained variance measures indicated that the models accounted for substantial variability in protection performance outcomes beyond control effects.

Table 9: Hierarchical Regression Results: Compliance Framework Maturity Predicting Outcomes with Controls

Outcome Model	Predictor	β (Std.)	t	p	R^2	ΔR^2 (Step 2)
Model A: Audit pass performance	Controls only (Step 1)	—	—	—	0.22	—
	Compliance maturity (Step 2)	0.46	8.21	<0.001	0.41	0.19
Model B: Audit finding severity	Controls only (Step 1)	—	—	—	0.18	—
	Compliance maturity (Step 2)	-0.49	-8.74	<0.001	0.42	0.24
Model C: Security incidents (count outcome)	Controls only (Step 1)	—	—	—	0.16	—
	Compliance maturity (Step 2)	-0.38	-6.52	<0.001	0.30	0.14
Model D: Data-handling violations (count outcome)	Controls only (Step 1)	—	—	—	0.20	—
	Compliance maturity (Step 2)	-0.44	-7.90	<0.001	0.38	0.18

Table 9 reported hierarchical regression outcomes showing that compliance framework maturity contributed substantial incremental explanatory power beyond controls. After adjusting for property size, transaction volume, workforce turnover, geographic region, and cloud adoption, compliance maturity remained statistically significant across all outcome models. The standardized coefficients indicated a strong positive relationship with audit pass performance and strong negative relationships with audit finding severity, security incident occurrence, and operational violation frequency. The R^2 change values indicated that adding compliance maturity materially improved model fit relative to control-only models. These results supported the hypotheses that higher compliance maturity aligned with stronger compliance assurance and reduced adverse security and operational handling outcomes.

Table 10: Moderation and Layer-Comparison Regression Results

Outcome	Key Predictors	β (Std.)	t	p	R^2
Audit pass performance	Compliance maturity	0.40	6.95	<0.001	0.46
	Maturity × integration complexity	0.14	2.41	0.017	
	Maturity × third-party dependency	0.11	2.02	0.045	
Security incidents	Compliance maturity	-0.31	-5.12	<0.001	0.35
	Maturity × integration complexity	-0.16	-2.76	0.006	
	Maturity × third-party dependency	-0.13	-2.30	0.022	
Layer comparison: Audit pass performance	Governance quality	0.33	4.98	<0.001	0.49
	Process execution strength	0.18	2.64	0.009	
	Technical control maturity	0.21	3.12	0.002	
Layer comparison: Data-handling violations	Governance quality	-0.19	-2.74	0.007	0.41
	Process execution strength	-0.34	-4.96	<0.001	
	Technical control maturity	-0.17	-2.51	0.013	

Table 10 summarized moderation and layer-comparison models. The interaction terms indicated that platform integration complexity and third-party dependency strengthened the relationship between compliance maturity and outcomes, showing that maturity had a larger protective association in more complex and vendor-exposed ecosystems. For audit pass performance, positive interaction coefficients indicated greater gains in audit performance under higher complexity and vendor exposure. For security incidents, negative interaction coefficients indicated stronger reduction in incident occurrence as maturity increased under higher complexity and vendor exposure. Layer comparison results indicated differentiated predictive strength, as governance quality showed the strongest association with audit outcomes, while process execution showed the strongest association with operational handling outcomes.

DISCUSSION

Digital compliance frameworks for protecting customer data across service and hospitality operations platforms were discussed in this study as an operational capability that was expressed through coordinated governance structures, disciplined process execution, and consistently deployed technical controls across interconnected systems (Line et al., 2020). The findings indicated that higher compliance framework maturity was associated with stronger compliance performance outcomes and reduced adverse protection outcomes, and this pattern aligned with earlier empirical and conceptual work that framed compliance as a management system rather than a standalone policy requirement. Prior research on information security governance had characterized maturity as the extent to which roles, policies, oversight routines, and technical safeguards were institutionalized and reinforced through evidence-producing practices, and the present results were consistent with that position by showing that maturity contributed material explanatory power beyond operational exposure controls. The observed association between compliance maturity and higher audit performance was coherent with audit and verification scholarship that treated assessment performance as an indicator of both control

presence and operational discipline, because audits typically evaluated not only technical safeguards but also documentation, accountability, and procedural consistency (Filimonau & Naumova, 2020). The negative association between compliance maturity and audit finding severity further suggested that mature frameworks were linked to fewer high-impact deficiencies, which aligned with earlier observations that systematic compliance systems reduced the likelihood of critical gaps across dispersed environments. The study also indicated that maturity was related to reductions in incident counts and operational handling violations, supporting the broader literature that linked structured governance and control environments to fewer realized risk events. Hospitality and service operations research had long emphasized that customer data moved across multiple operational systems and across property boundaries, and this ecosystem characteristic made consistency in implementation a central determinant of protective outcomes. The present findings extended that logic quantitatively by showing that maturity explained meaningful variance after controlling for property size, transaction intensity, turnover, geographic context, and cloud adoption, suggesting that capability mattered even under differing operational conditions. These results were also consistent with earlier insights that compliance effectiveness required integration with operational realities, because customer data protection in hospitality occurred at high-frequency touchpoints such as booking, check-in, payment, and guest communication, where control breakdowns could occur if compliance was treated as separate from service delivery (Paraskevas, 2020). Accordingly, the study supported an interpretation of digital compliance frameworks as a measurable organizational capability that was associated with both assurance outcomes and event-based protection outcomes across service and hospitality platform environments.

The discussion of audit-related outcomes highlighted how governance and evidence practices operated as central drivers of compliance performance in service and hospitality contexts. The study found that compliance maturity was positively related to audit pass performance and negatively related to the severity of audit findings, which corresponded with earlier work that described audits as structured tests of control design, control operation, and documentation quality (X. Hu et al., 2021). Prior studies of compliance programs had indicated that organizations with stronger accountability structures and more disciplined evidence repositories tended to perform better under assessment regimes because they could demonstrate control execution, exception handling, and remediation actions with clear traceability. The present results were consistent with that pattern and further implied that audit performance in hospitality environments reflected more than technical configurations alone. In operational settings where multiple properties shared platforms or policies yet varied in staffing stability and local practices, audit performance tended to reflect how effectively corporate requirements were translated into property routines and platform configurations. Earlier research on distributed operations had emphasized that variability in local execution often produced repeated findings across sites, particularly when responsibility boundaries were unclear or when properties relied on informal workarounds under service pressure. The observed association between higher compliance maturity and lower finding severity aligned with that earlier position because mature frameworks were expected to reduce both inconsistency and weak documentation, limiting the conditions that produced high-severity findings (Shukla et al., 2022). The study's findings also indicated that remediation timelines moved with maturity, which matched earlier observations that remediation performance depended on control ownership, prioritization discipline, and the ability to coordinate with vendors and platform owners across the ecosystem. In hospitality technology environments, remediation often required coordinated action among corporate IT, property operations, and third-party providers, and earlier work had suggested that such coordination was faster where governance was clear and where evidence supported precise identification of control breakdowns. The present results were consistent with this view by indicating that maturity related to improved compliance outcomes in a way that was robust to exposure controls. This interpretation supported an understanding of audit performance as a composite reflection of governance quality, process reliability, and the documentation infrastructure needed to demonstrate compliance across platforms and properties (Lau, 2020). The discussion therefore positioned audit outcomes as meaningful indicators of compliance framework effectiveness in hospitality settings, particularly where external scrutiny and standards-based requirements demanded repeatable evidence and timely closure of deficiencies.

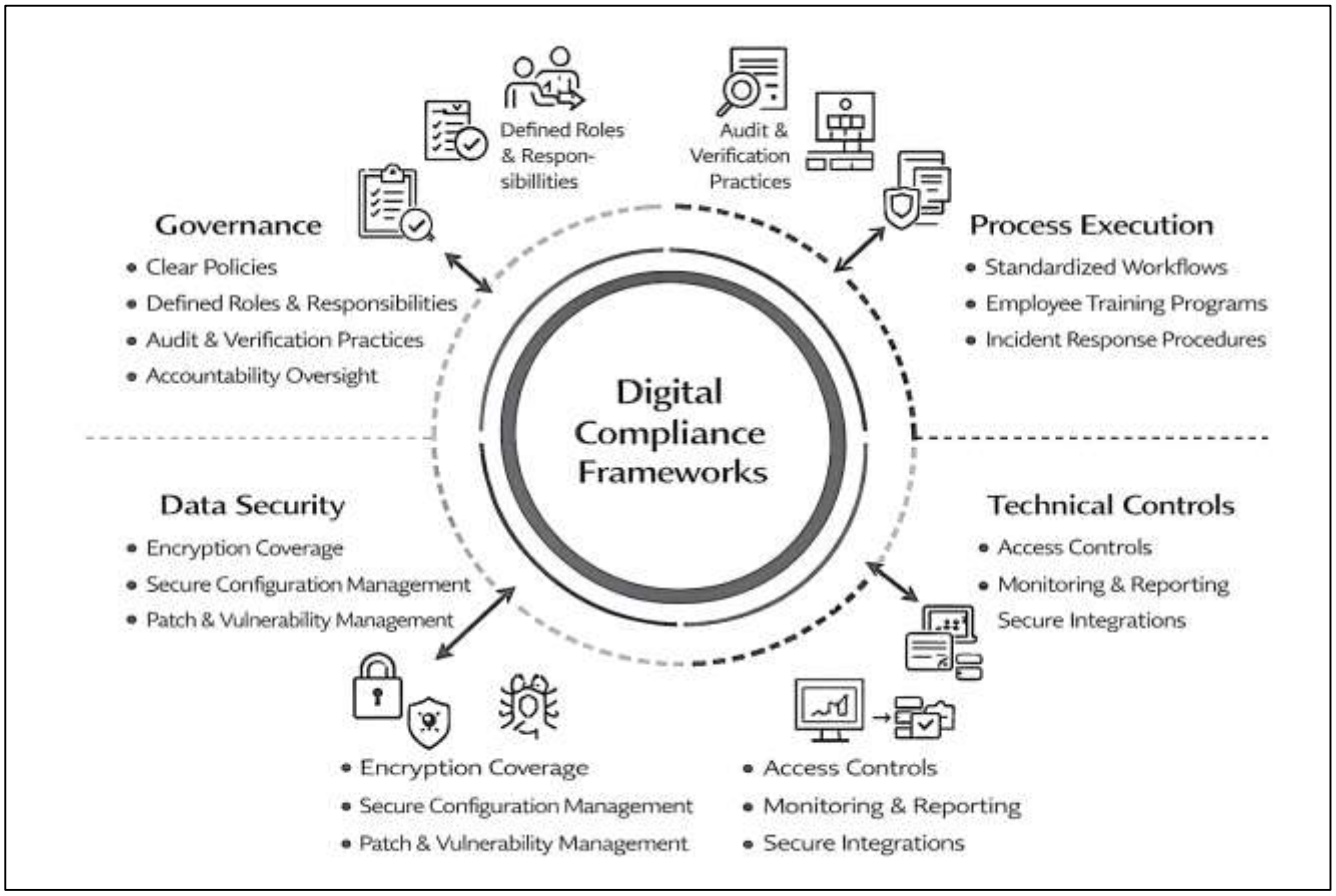
Security outcomes were discussed as realized indicators of protection performance that complemented audit assurance measures, and the study found that higher compliance maturity was associated with fewer security incidents and fewer unauthorized access events. Earlier research on cyber risk had emphasized that incident frequency and access misuse were influenced by both technical vulnerabilities and operational behaviors, especially in environments with complex platform ecosystems and high workforce variability (Bonfanti et al., 2021). The present findings aligned with those perspectives by suggesting that mature compliance frameworks were linked to fewer adverse security events after adjusting for property size, transaction volume, turnover, geography, and cloud adoption. This pattern also corresponded with earlier work on layered security governance that treated effective protection as the product of technical controls, disciplined access processes, monitoring visibility, and response readiness (Ahmad et al., 2021). The reduction in incidents associated with higher maturity was consistent with the idea that encryption coverage, secure configuration discipline, patch management timeliness, and least-privilege practices reduced exploitability, while monitoring and logging practices increased detection capability and deterrence. Earlier scholarship had also pointed to privileged access as a recurrent source of high-impact incidents, and the study's broader process-and-technical framing supported an interpretation that mature environments managed privileged access more consistently, contributing to reduced unauthorized access events. Hospitality-specific research had described operational pressures such as high guest volume and fast service cycles, which increased reliance on shared devices, rapid shift handovers, and frequent account provisioning, all of which had been associated with higher access risk in earlier studies. The present results did not contradict that operational reality; rather, they suggested that maturity reduced the translation of these pressures into incident outcomes by strengthening process discipline and technical safeguards. In addition, earlier work had highlighted that incident counts could reflect both true risk and detection capability, since more mature environments sometimes detected and recorded more events (Baloch et al., 2022). The negative association observed in this study suggested that the maturity construct captured more than detection alone and aligned more with reduction in realized adverse events, or that improved discipline reduced the number of significant events that met incident thresholds. This interpretation remained consistent with the broader literature that framed mature security and compliance programs as reducing both exposure and the probability of successful exploitation through systematic control coverage and oversight. The discussion therefore positioned security outcomes as an essential outcome domain for evaluating compliance frameworks in hospitality contexts because operational platforms handled high volumes of sensitive data and because incidents directly threatened customer trust, financial integrity, and service continuity (Kopalle et al., 2020). By demonstrating a measurable relationship between maturity and incident-related outcomes, the study reinforced earlier theoretical claims that compliance capability functioned as a practical risk-reduction mechanism in complex service ecosystems.

Operational data handling outcomes were discussed as a behavioral and procedural dimension of customer data protection performance, and the study found that higher compliance maturity was associated with lower levels of data-handling violations and fewer operational deviations from prescribed practices (Ranchordás & Goanta, 2020). This result aligned with earlier work in information security compliance and organizational behavior that emphasized the central role of employee adherence, perceived feasibility, and normative reinforcement in determining whether rules were followed in daily work. Hospitality and service environments had been repeatedly characterized in prior research as high-interaction, time-sensitive settings where frontline personnel handled identity and payment information under pressure and where procedural shortcuts could emerge when systems or policies were perceived as slow or burdensome. The present findings suggested that mature compliance frameworks were associated with reductions in such violations, which was consistent with earlier studies that linked clear roles, consistent training, and enforceable procedures to stronger compliance behavior. Operational handling outcomes also reflected the effectiveness of workflow design and policy integration into service processes, a theme emphasized in service operations research that treated routine work design as a determinant of performance consistency. Where compliance policies were aligned with operational reality and where employees were trained to apply them under typical service constraints, earlier studies had indicated that violations decreased because staff relied

less on workarounds (Rahmadian et al., 2023). The present results were consistent with this interpretation by showing that compliance maturity related to lower violation outcomes even after accounting for turnover and operational exposure, both of which had been identified as risk drivers in earlier hospitality workforce literature. This pattern suggested that mature frameworks created stability through standardized onboarding and training routines, clear access procedures, and structured incident and exception escalation pathways that reduced informal handling of customer data. The discussion also considered that operational violations frequently occurred at platform boundaries, such as when customer information was transferred to external partners, shared across departments, or communicated through messaging tools. Earlier studies had indicated that these boundary activities were vulnerable to improper sharing and inconsistent documentation, particularly when vendor and integration complexity increased. The present findings implied that maturity constrained these vulnerabilities by reinforcing consistent processes and by providing evidence-based oversight that discouraged informal data movement. This interpretation aligned with earlier governance scholarship that treated documentation and monitoring as behavior-shaping mechanisms because they increased the perceived visibility and accountability of actions (Ait Bennacer et al., 2022). In hospitality contexts where customer data could be mishandled through routine practices rather than deliberate misuse, the study supported a discussion that positioned operational handling outcomes as critical indicators of compliance framework effectiveness and as a complementary domain alongside audit and security incident outcomes.

Moderation findings were discussed to interpret how platform ecosystem complexity and third-party dependency conditioned the relationship between compliance maturity and customer data protection outcomes. The study found that the association between maturity and protection performance changed under higher levels of integration complexity and vendor exposure, and this pattern aligned with earlier research that described complex, interconnected ecosystems as amplifiers of both exposure and compliance burden (Semantha et al., 2021). Prior work on hospitality technology ecosystems had emphasized that increasing interoperability and reliance on external platforms expanded data pathways and created more points at which configuration errors, interface weaknesses, and inconsistent authorization controls could appear. Outsourcing and supply-chain risk research had similarly highlighted that third-party involvement increased attack surface and reduced direct organizational visibility, making consistent governance and control oversight more difficult. In this context, the finding that complexity and vendor dependency altered the maturity-outcome relationship suggested that maturity operated as a compensatory capability that became more consequential when exposure was higher. Earlier governance literature had argued that complex environments required stronger coordination, clearer responsibility allocation, and more disciplined monitoring because fragmented ownership increased the risk of control gaps (Susanto et al., 2021). The present results were consistent with that claim by indicating that the protective association of maturity was more pronounced in settings characterized by heavy integration and vendor access. This interpretation also aligned with earlier security management perspectives that treated complexity as a multiplier of uncertainty, requiring stronger evidence practices and more systematic control coverage to maintain stable performance. Vendor dependency introduced additional coordination requirements for incident response, remediation, and evidence gathering, and earlier studies had noted that organizations with weak vendor governance experienced delayed mitigation and incomplete documentation, increasing both risk and audit vulnerability. The present findings supported a discussion that framed vendor exposure as not merely additive risk but as a contextual factor that reshaped how internal compliance capability translated into outcomes. Integration complexity also influenced how quickly control drift could occur, as platform changes and new connections could undermine established baselines unless continuous monitoring and configuration management were strong. The study's moderation results were compatible with earlier observations that maturity reduced the likelihood that complexity translated into severe outcomes by strengthening operational discipline and technical safeguards (Wang et al., 2022). This discussion reinforced the importance of including ecosystem characteristics in compliance effectiveness models because hospitality operations did not occur in a single-system environment, and the effectiveness of frameworks depended on how well controls scaled across interdependent platforms and third-party relationships.

Figure 12: Digital Compliance Outcomes Framework Model



Comparative pathway findings were discussed to interpret the differentiated roles of governance, process execution, and technical controls in predicting distinct outcome domains. The study found that governance quality demonstrated stronger associations with audit-related outcomes, process execution demonstrated stronger associations with operational handling outcomes, and technical controls demonstrated stronger associations with security outcomes (Garrido-Moreno et al., 2021). This differentiated pattern aligned with earlier layered governance and control theories that emphasized distinct causal mechanisms: governance established accountability and standardization, process execution determined the reliability of routine behavior, and technical controls constrained exploitability and strengthened detection. Earlier audit-focused research had emphasized that governance structures and documentation practices shaped assessment performance because audits evaluated policy coverage, evidence availability, role clarity, and the discipline of reviews and approvals, in addition to technical safeguards. Therefore, the stronger association of governance with audit outcomes was consistent with earlier work that treated audit performance as a reflection of organizational oversight capability. Process execution's stronger association with operational handling outcomes aligned with earlier behavioral compliance studies that linked adherence to training, role-based procedures, access workflows, and the feasibility of policies in frontline operations. In hospitality, process execution included onboarding and offboarding discipline, access review routines, training coverage, incident escalation compliance, and retention workflow execution, all of which had been emphasized in earlier studies as determinants of day-to-day compliance behavior under service pressure (Mondal et al., 2023). Technical controls' stronger relationship with security outcomes corresponded with earlier security engineering and risk research that emphasized encryption coverage, configuration baselines, patch management discipline, monitoring completeness, and segmentation as determinants of incident probability and unauthorized access outcomes. Earlier scholarship had also suggested that technical controls provided necessary constraints but could be undermined if process execution was weak; the present differentiated findings did not contradict this interaction logic, but rather showed that, when modeled simultaneously, each layer aligned more strongly with the outcome

domain most directly connected to its mechanism. This discussion supported the interpretation that compliance frameworks should be evaluated and strengthened as layered systems, because improvements in one layer were unlikely to fully substitute for weaknesses in another. The observed differentiated associations further supported the study's quantitative framing of compliance maturity as a multidimensional construct that captured system-like capability rather than a single-factor explanation (Koohang et al., 2023). In hospitality operations platforms where customer data flowed across multiple systems and service touchpoints, the differentiated pathways highlighted why a comprehensive evaluation of governance, processes, and technical controls was necessary to explain performance across audit, incident, and operational handling outcomes.

The overall discussion synthesized how the study's models accounted for substantial variability in customer data protection outcomes after controls were included, reinforcing the conclusion that compliance frameworks represented meaningful explanatory factors beyond operational exposure and contextual differences (Hsieh et al., 2021). Earlier service operations research had highlighted that larger properties and higher transaction intensity increased exposure simply by increasing the number of interactions and the volume of data processed, and the inclusion of property size and transaction volume as controls acknowledged that baseline risk varied with operational scale. Workforce turnover had been consistently treated in hospitality literature as a driver of instability in training coverage and access governance, and its inclusion as a control reflected the sector's structural workforce realities. Geographic and deployment context, including region and cloud adoption level, had been discussed in earlier studies as sources of variation in compliance workload, platform standardization, and monitoring capabilities, and the control structure recognized these differences. Despite these contextual influences, compliance maturity retained strong associations with outcomes, supporting earlier theoretical positions that organizational capability shaped protection performance even under varying exposure. The moderation and layer-comparison results further strengthened this interpretation by showing that capability was not uniform in its effects across environments or outcome domains. The discussion therefore interpreted digital compliance frameworks in hospitality as operational systems whose performance depended on the interplay of governance, process execution, and technical controls within an ecosystem shaped by integrations, vendors, and governance structure (Gómez-Carmona et al., 2023). Prior research had frequently characterized hospitality technology as an ecosystem where interoperability created both value and vulnerability, and the present findings provided quantitative reinforcement that protection performance varied systematically with both internal capability and ecosystem conditions. By comparing the observed relationships with earlier streams of research on governance, security controls, compliance behavior, auditing, and platform ecosystems, the discussion positioned the study as consistent with established theoretical claims while providing a structured, outcomes-based quantitative framing. In this way, the study was discussed as offering empirical confirmation that stronger compliance framework maturity aligned with better audit performance and fewer adverse events across security and operational handling domains in service and hospitality operations platforms (Butt, 2020).

CONCLUSION

Digital Compliance Frameworks for Protecting Customer Data Across Service and Hospitality Operations Platforms were discussed as an integrated operational capability that shaped measurable protection performance across platform ecosystems where customer information was continuously collected, transferred, stored, and reused during service delivery. In this study, compliance frameworks were treated as structured systems rather than static policy documents, meaning that protection outcomes were understood as the result of coordinated governance arrangements, disciplined process execution, and consistently deployed technical safeguards across interconnected operational platforms. The hospitality and service context were characterized by high-volume customer interactions, frequent workforce transitions, and extensive reliance on third-party platforms, which collectively increased both exposure and the difficulty of sustaining uniform control performance across properties and systems. The findings indicated that higher compliance framework maturity was associated with stronger compliance performance and lower adverse outcomes, reflecting a pattern that was coherent with earlier evidence that organizational control environments produced verifiable differences in audit results, incident occurrence, and operational handling behaviors. Compliance performance indicators,

including stronger audit results and lower severity of assessment findings, were interpreted as evidence that mature frameworks supported both control implementation and documentation discipline, which remained central to demonstrability in regulated and standards-driven environments. Security outcomes were also interpreted as realized indicators of protection performance because reductions in incidents and unauthorized access events signaled that mature control environments constrained exploitability and strengthened operational safeguards in platforms that handled identity and payment information. Operational handling outcomes further reinforced this interpretation by showing that mature frameworks corresponded with fewer policy violations and improper sharing events, consistent with earlier behavioral compliance research that linked role clarity, training coverage, and routine enforcement to stronger adherence under time pressure. The study also highlighted that ecosystem conditions shaped performance, because integration complexity and third-party dependency increased exposure and created more points where control gaps could emerge, aligning with prior scholarship that described hospitality technology as an ecosystem in which interoperability generated both value and vulnerability. Differentiated pathways were also observed across framework layers, with governance demonstrating stronger relationships with audit outcomes, process execution demonstrating stronger relationships with operational handling outcomes, and technical controls demonstrating stronger relationships with incident outcomes, supporting earlier layered security and governance theories that emphasized distinct mechanisms connecting controls to performance domains. After adjusting for operational scale, transaction intensity, turnover, region, and cloud adoption, compliance maturity retained explanatory power, which suggested that protection performance varied systematically with internal capability beyond differences in exposure. Overall, Digital Compliance Frameworks for Protecting Customer Data Across Service and Hospitality Operations Platforms were positioned as measurable, multi-layered systems that influenced assurance outcomes and reduced adverse protection events in complex operational environments where customer trust, service continuity, and data accountability remained tightly linked.

RECOMMENDATION

Recommendations for strengthening Digital Compliance Frameworks for Protecting Customer Data Across Service and Hospitality Operations Platforms should be structured as an operational program that reinforces governance, process execution, and technical controls in a coordinated manner across all properties, platforms, and vendor relationships. A first recommendation emphasized formal accountability alignment by ensuring that compliance ownership, security ownership, platform ownership, and property-level stewardship were explicitly assigned and consistently documented across the organization, because clear responsibility reduced ambiguity in approvals, exception handling, incident escalation, and evidence production. A second recommendation focused on policy architecture standardization by maintaining a unified policy set that covered access control, acceptable use, retention and deletion, incident response, and vendor oversight, and by ensuring that policy updates were managed through disciplined review cycles aligned with platform changes, vendor onboarding, and audit feedback. A third recommendation emphasized evidence readiness through centralized documentation practices that ensured logs, training records, risk assessments, approvals, and remediation records remained accessible, complete, and consistently retained across properties, enabling faster audits and more defensible incident investigations. A fourth recommendation addressed identity and access lifecycle execution by tightening onboarding and offboarding routines, enforcing role-based access mapped to operational job functions, requiring approvals and periodic validation for privileged access, and ensuring that access changes were completed rapidly and recorded in auditable workflows, particularly in high-turnover environments typical of hospitality operations. A fifth recommendation centered on workforce compliance by embedding data protection behaviors into operational training and shift routines, requiring documented completion for all staff who interacted with customer data, using comprehension checks to confirm policy understanding, and reinforcing adherence through visible managerial support and consistent enforcement that minimized informal workarounds. A sixth recommendation prioritized incident response readiness by maintaining defined triage pathways, clear escalation thresholds, and coordinated vendor response procedures, supported by continuous monitoring and evidence capture so that detection and containment actions were executed quickly and consistently across properties. A seventh

recommendation focused on retention and deletion execution by maintaining accurate data inventories across platforms, applying retention rules consistently, processing deletion requests through structured workflows, and ensuring backups were handled in ways that supported compliance with retention limits and accountability requirements. A final recommendation emphasized that platform ecosystem complexity and vendor exposure required strengthened integration governance, including documented interface inventories, security validation for new integrations, contractual safeguards that specified vendor responsibilities for customer data protection, and routine vendor assessments that matched the sensitivity and breadth of shared data. Collectively, these recommendations positioned compliance as a measurable operational capability embedded into platform management and service delivery routines across hospitality ecosystems where customer data moved across multiple systems, properties, and external providers.

LIMITATIONS

Limitations associated with this study on Digital Compliance Frameworks for Protecting Customer Data Across Service and Hospitality Operations Platforms primarily reflected constraints related to research design, measurement conditions, data availability, and contextual generalizability across heterogeneous operational environments. The quantitative design relied on cross-sectional measurement, which restricted the ability to establish temporal ordering among compliance framework maturity, ecosystem complexity, and customer data protection performance outcomes, even though the statistical models controlled for key operational exposure variables. The study's measurement approach also faced limitations arising from mixed-source indicators that combined survey-based construct assessments with operational records, because properties varied in the completeness, consistency, and standardization of audit reports, incident logs, and policy violation documentation. Differences in how incidents were defined and recorded across properties could have introduced measurement variability, particularly when some sites maintained stronger detection and reporting practices than others, creating the possibility that higher monitoring capability increased recorded incident counts even when underlying risk was lower. Survey-based measures of governance quality, process execution discipline, and technical control maturity were also subject to perceptual bias and social desirability effects, especially in regulated contexts where respondents might have perceived value in presenting compliance practices more favorably. Although aggregation across respondents and triangulation with available operational metrics reduced reliance on single-source perceptions, the possibility of common-method influence could not be fully eliminated where objective operational records were incomplete or unavailable for certain properties. The study also relied on property-level aggregation, which limited the ability to capture platform-level variations in control configuration within the same property, such as differences between payment environments and guest engagement platforms, and this aggregation may have reduced sensitivity to localized technical weaknesses that occurred within specific systems. Furthermore, platform ecosystem complexity and third-party dependency were represented through structured inventory-based indicators that captured breadth and interconnectedness, yet these measures could not fully represent qualitative differences in integration security, vendor control maturity, or contractual enforcement strength, which may have influenced outcomes beyond what count-based exposure indicators captured. The sample context introduced additional constraints because service and hospitality properties differed in operating models, including corporate-owned, managed, and franchised arrangements, which influenced governance authority and resource allocation, and these differences could have affected compliance execution in ways not fully captured by the included controls. Geographic variation also imposed limits, as properties operating under different regulatory regimes and cultural expectations may have experienced different baseline compliance burdens and documentation practices, and the analysis could not fully isolate jurisdiction-specific effects when data were pooled across regions. Finally, the study focused on measurable outcomes such as audit performance, incident occurrence, and policy violations, which were important indicators of protection performance, yet these outcomes could not fully capture customer perceptions of trust,

reputational impacts, or indirect operational disruptions associated with security events, indicating that the dependent variable represented a partial view of broader customer data protection consequences in hospitality operations.

REFERENCES

[1]. Aase, K., & Waring, J. (2020). Crossing boundaries: establishing a framework for researching quality and safety in care transitions. *Applied ergonomics*, *89*, 103228.

[2]. Abdul, K. (2023). Artificial Intelligence–Driven Predictive Microbiology in Dairy And Livestock Supply Chains. *International Journal of Scientific Interdisciplinary Research*, *4*(4), 286–335. https://doi.org/10.63125/syj6pp52

[3]. Ahmad, R. W., Salah, K., Jayaraman, R., Hasan, H. R., Yaqoob, I., & Omar, M. (2021). The role of blockchain technology in aviation industry. *IEEE Aerospace and Electronic Systems Magazine*, *36*(3), 4-15.

[4]. Ait Bennacer, S., Aaroud, A., Sabiri, K., Rguibi, M. A., & Cherradi, B. (2022). Design and implementation of a New Blockchain-based digital health passport: A Moroccan case study. *Informatics in Medicine Unlocked*, *35*, 101125.

[5]. Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., & Rahman, M. S. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future generation computer systems*, *95*, 511-521.

[6]. Alaneme George, U., & Mbadike Elvis, M. (2019). Modelling of the mechanical properties of concrete with cement ratio partially replaced by aluminium waste and sawdust ash using artificial neural network. *SN Applied Sciences*, *1*(11), 1514.

[7]. Alt, R. (2021). Electronic Markets on platform complexity. *Electronic markets*, *31*(4), 737-742.

[8]. Ariono, B., Wasesa, M., & Dhewanto, W. (2022). The drivers, barriers, and enablers of building information modeling (BIM) innovation in developing countries: Insights from systematic literature review and comparative analysis. *Buildings*, *12*(11), 1912.

[9]. Aulkemeier, F., Iacob, M.-E., & van Hillegersberg, J. (2019). Platform-based collaboration in digital ecosystems. *Electronic markets*, *29*(4), 597-608.

[10]. Badi, S., & Murtagh, N. (2019). Green supply chain management in construction: A systematic literature review and future research agenda. *Journal of cleaner production*, *223*, 312-322.

[11]. Baloch, Q. B., Maher, S., Shah, S. N., Sheeraz, M., Iqbal, N., & Raza, H. (2022). Revitalization of tourism and hospitality sector: preempting pandemics through lessons learned. *Environmental science and pollution research*, *29*(55), 83099-83111.

[12]. Beach, T. H., Hippolyte, J.-L., & Rezgui, Y. (2020). Towards the adoption of automated regulatory compliance checking in the built environment. *Automation in construction*, *118*, 103285.

[13]. Bera, B., Saha, S., & Bhattacharjee, S. (2020). Forest cover dynamics (1998 to 2019) and prediction of deforestation probability using binary logistic regression (BLR) model of Silabati watershed, India. *Trees, Forests and People*, *2*, 100034.

[14]. Bhavsar, V., Sridharan, S. R., & Sudarsan, J. (2023). Barriers to circular economy practices during construction and demolition waste management in an emerging economy. *Resources, Conservation & Recycling Advances*, *20*, 200198.

[15]. Bonfanti, A., Vigolo, V., & Yfantidou, G. (2021). The impact of the Covid-19 pandemic on customer experience design: The hotel managers' perspective. *International Journal of Hospitality Management*, *94*, 102871.

[16]. Borie, M., Mahony, M., Obermeister, N., & Hulme, M. (2021). Knowing like a global expert organization: Comparative insights from the IPCC and IPBES. *Global Environmental Change*, *68*, 102261.

[17]. Borsatto, J. M. L. S., & Bazani, C. L. (2021). Green innovation and environmental regulations: A systematic review of international academic works. *Environmental science and pollution research*, *28*(45), 63751-63768.

[18]. Buhalis, D., & Sinarta, Y. (2019). Real-time co-creation and nowness service: lessons from tourism and hospitality. *Journal of Travel & Tourism Marketing*, *36*(5), 563-582.

[19]. Burdon, W. M., & Sorour, M. K. (2020). Institutional theory and evolution of 'a legitimate'compliance culture: The case of the UK financial service sector. *Journal of Business Ethics*, *162*(1), 47-80.

[20]. Butt, J. (2020). A conceptual framework to support digital transformation in manufacturing using an integrated business process management approach. *Designs*, *4*(3), 17.

[21]. Carrera-Rivera, A., Ochoa, W., Larrinaga, F., & Lasa, G. (2022). How-to conduct a systematic literature review: A quick guide for computer science research. *MethodsX*, *9*, 101895.

[22]. Casado-Vara, R., Chamoso, P., De la Prieta, F., Prieto, J., & Corchado, J. M. (2019). Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management. *Information Fusion*, *49*, 227-239.

[23]. Cenamor, J. (2021). Complementor competitive advantage: A framework for strategic decisions. *Journal of Business Research*, *122*, 335-343.

[24]. Chen, Y., Zhang, Y., & Zhou, B. (2020). Research on the risk of block chain technology in Internet finance supported by wireless network. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1), 71.

[25]. Cheng, M., & Jin, X. (2019). What do Airbnb users care about? An analysis of online review comments. *International Journal of Hospitality Management*, *76*, 58-70.

[26]. Choi, H., & Kandampully, J. (2019). The effect of atmosphere on customer engagement in upscale hotels: An application of SOR paradigm. *International Journal of Hospitality Management*, *77*, 40-50.

[27]. Chouaibi, S., Festa, G., Quaglia, R., & Rossi, M. (2022). The risky impact of digital transformation on organizational performance–evidence from Tunisia. *Technological Forecasting and Social Change*, *178*, 121571.

[28]. Couclelis, H. (2020). Towards an operational typology of geographic entities with ill-defined boundaries. In *Geographic objects with indeterminate boundaries* (pp. 45-55). CRC Press.

[29]. Cui, H., Li, F., & Tomsovic, K. (2020). Hybrid symbolic-numeric framework for power system modeling and analysis. *IEEE Transactions on Power Systems*, *36*(2), 1373-1384.
[30]. Danese, P., Lion, A., & Vinelli, A. (2019). Drivers and enablers of supplier sustainability practices: a survey-based analysis. *International Journal of Production Research*, *57*(7), 2034-2056.
[31]. Fasoulis, I., & Kurt, R. E. (2019). Determinants to the implementation of corporate social responsibility in the maritime industry: a quantitative study. *Journal of International Maritime Safety, Environmental Affairs, and Shipping*, *3*(1-2), 10-20.
[32]. Fernando, Y., Tseng, M.-L., Wahyuni-Td, I. S., de Sousa Jabbour, A. B. L., Chiappetta Jabbour, C. J., & Foropon, C. (2023). Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in Malaysia. *Journal of Industrial and Production Engineering*, *40*(2), 102-116.
[33]. Filimonau, V., & Naumova, E. (2020). The blockchain technology and the scope of its application in hospitality operations. *International Journal of Hospitality Management*, *87*, 102383.
[34]. Floetgen, R. J., Strauss, J., Weking, J., Hein, A., Urmetzer, F., Böhm, M., & Krcmar, H. (2021). Introducing platform ecosystem resilience: leveraging mobility platforms and their ecosystems for the new normal during COVID-19. *European Journal of Information Systems*, *30*(3), 304-321.
[35]. Font, X., English, R., Gkritzali, A., & Tian, W. S. (2021). Value co-creation in sustainable tourism: A service-dominant logic approach. *Tourism Management*, *82*, 104200.
[36]. Fuchs, H., Aghajanzadeh, A., & Therkelsen, P. (2020). Identification of drivers, benefits, and challenges of ISO 50001 through case study content analysis. *Energy policy*, *142*, 111443.
[37]. Gamidullaeva, L., Tolstykh, T., Bystrov, A., Radaykin, A., & Shmeleva, N. (2021). Cross-sectoral digital platform as a tool for innovation ecosystem development. *Sustainability*, *13*(21), 11686.
[38]. Garrido-Moreno, A., Garcia-Morales, V. J., & Martin-Rojas, R. (2021). Going beyond the curve: Strategic measures to recover hotel activity in times of COVID-19. *International Journal of Hospitality Management*, *96*, 102928.
[39]. Geldenhuys, M., Gaigher, R., Pryke, J., & Samways, M. (2021). Diverse herbaceous cover crops promote vineyard arthropod diversity across different management regimes. *Agriculture, Ecosystems & Environment*, *307*, 107222.
[40]. Golan, M. S., Jernegan, L. H., & Linkov, I. (2020). Trends and applications of resilience analytics in supply chain modeling: systematic literature review in the context of the COVID-19 pandemic. *Environment Systems and Decisions*, *40*(2), 222-243.
[41]. Gómez-Carmona, O., Buján-Carballal, D., Casado-Mansilla, D., López-de-Ipiña, D., Cano-Benito, J., Cimmino, A., Poveda-Villalón, M., García-Castro, R., Almela-Miralles, J., & Apostolidis, D. (2023). Mind the gap: The AURORAL ecosystem for the digital transformation of smart communities and rural areas. *Technology in Society*, *74*, 102304.
[42]. González-Serrano, L., Talón-Ballestero, P., Muñoz-Romero, S., Soguero-Ruiz, C., & Rojo-Álvarez, J. L. (2019). Entropic statistical description of big data quality in hotel customer relationship management. *Entropy*, *21*(4), 419.
[43]. González-Serrano, L., Talón-Ballestero, P., Muñoz-Romero, S., Soguero-Ruiz, C., & Rojo-Álvarez, J. L. (2020). A big data approach to customer relationship management strategy in hospitality using multiple correspondence domain description. *Applied Sciences*, *11*(1), 256.
[44]. Hammad, S., & Md Sarwar Hossain, S. (2025). Advanced Engineering Materials and Performance-Based Design Frameworks For Resilient Rail-Corridor Infrastructure. *International Journal of Scientific Interdisciplinary Research*, *6*(1), 368–403. https://doi.org/10.63125/c3g3sx44
[45]. Hammad, S., & Muhammad Mohiul, I. (2023). Geotechnical And Hydraulic Simulation Models for Slope Stability And Drainage Optimization In Rail Infrastructure Projects. *Review of Applied Science and Technology*, *2*(02), 01–37. https://doi.org/10.63125/jmx3p851
[46]. Hamzei, E., Winter, S., & Tomko, M. (2020). Place facets: a systematic literature review. *Spatial Cognition & Computation*, *20*(1), 33-81.
[47]. Han, Y., Chong, W. K., & Li, D. (2020). A systematic literature review of the capabilities and performance metrics of supply chain resilience. *International Journal of Production Research*, *58*(15), 4541-4566.
[48]. Hang, L., & Kim, D.-H. (2019). Design and implementation of an integrated iot blockchain platform for sensing data integrity. *sensors*, *19*(10), 2228.
[49]. Hanif, Y., & Lallie, H. S. (2021). Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM-with perceived cyber security, risk, and trust. *Technology in Society*, *67*, 101693.
[50]. Hein, A., Schreieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Böhm, M., & Krcmar, H. (2020). Digital platform ecosystems. *Electronic markets*, *30*(1), 87-98.
[51]. Hein, A., Weking, J., Schreieck, M., Wiesche, M., Böhm, M., & Krcmar, H. (2019). Value co-creation practices in business-to-business platform ecosystems. *Electronic markets*, *29*(3), 503-518.
[52]. Howard, J., & Gugger, S. (2020). Fastai: a layered API for deep learning. *Information*, *11*(2), 108.
[53]. Hsieh, Y. J., Chen, Y.-L., & Wang, Y.-C. (2021). Government and social trust vs. hotel response efficacy: A protection motivation perspective on hotel stay intention during the COVID-19 pandemic. *International Journal of Hospitality Management*, *97*, 102991.
[54]. Hu, S., Xiong, C., Yang, M., Younes, H., Luo, W., & Zhang, L. (2021). A big-data driven approach to analyzing and modeling human mobility trend under non-pharmaceutical interventions during COVID-19 pandemic. *Transportation Research Part C: Emerging Technologies*, *124*, 102955.
[55]. Hu, X., Yan, H., Casey, T., & Wu, C.-H. (2021). Creating a safe haven during the crisis: How organizations can achieve deep compliance with COVID-19 safety measures in the hospitality industry. *International Journal of Hospitality Management*, *92*, 102662.

[56]. Hultin, L. (2019). On becoming a sociomaterial researcher: Exploring epistemological practices grounded in a relational, performative ontology. *Information and Organization*, *29*(2), 91-104.
[57]. Jabed Hasan, T., & Waladur, R. (2023). AI-Driven Cybersecurity, IOT Networking, And Resilience Strategies For Industrial Control Systems: A Systematic Review For U.S. Critical Infrastructure Protection. *International Journal of Scientific Interdisciplinary Research*, *4*(4), 144–176. https://doi.org/10.63125/mbyhj941
[58]. Jiménez, A., Saikia, P., Giné, R., Avello, P., Leten, J., Liss Lymer, B., Schneider, K., & Ward, R. (2020). Unpacking water governance: A framework for practitioners. *Water*, *12*(3), 827.
[59]. Jinnat, A., & Md. Kamrul, K. (2021). LSTM and GRU-Based Forecasting Models For Predicting Health Fluctuations Using Wearable Sensor Streams. *American Journal of Interdisciplinary Studies*, *2*(02), 32-66. https://doi.org/10.63125/1p8gbp15
[60]. Kansakar, P., Munir, A., & Shabani, N. (2019). Technology in the hospitality industry: Prospects and challenges. *IEEE Consumer Electronics Magazine*, *8*(3), 60-65.
[61]. Keszey, T. (2020). Behavioural intention to use autonomous vehicles: Systematic review and empirical extension. *Transportation Research Part C: Emerging Technologies*, *119*, 102732.
[62]. Kim, Y.-J., & Kim, H.-S. (2022). The impact of hotel customer experience on customer satisfaction through online reviews. *Sustainability*, *14*(2), 848.
[63]. Koohang, A., Nord, J. H., Ooi, K.-B., Tan, G. W.-H., Al-Emran, M., Aw, E. C.-X., Baabdullah, A. M., Buhalis, D., Cham, T.-H., & Dennis, C. (2023). Shaping the metaverse into reality: a holistic multidisciplinary understanding of opportunities, challenges, and avenues for future investigation. *Journal of Computer Information Systems*, *63*(3), 735-765.
[64]. Kopalle, P. K., Kumar, V., & Subramaniam, M. (2020). How legacy firms can embrace the digital ecosystem via digital customer orientation. *Journal of the Academy of Marketing Science*, *48*(1), 114-131.
[65]. Kumar, Y., Koul, A., Singla, R., & Ijaz, M. F. (2023). Artificial intelligence in disease diagnosis: a systematic literature review, synthesizing framework and future research agenda. *Journal of ambient intelligence and humanized computing*, *14*(7), 8459-8486.
[66]. Kutub Uddin, A., Md Mostafizur, R., Afrin Binta, H., & Maniruzzaman, B. (2022). Forecasting Future Investment Value with Machine Learning, Neural Networks, And Ensemble Learning: A Meta-Analytic Study. *Review of Applied Science and Technology*, *1*(02), 01-25. https://doi.org/10.63125/edxgjg56
[67]. Lai, I. K. W. (2019). Hotel image and reputation on building customer loyalty: An empirical study in Macau. *Journal of Hospitality and tourism Management*, *38*, 111-121.
[68]. Lau, A. (2020). New technologies used in COVID-19 for business survival: Insights from the Hotel Sector in China. *Information Technology & Tourism*, *22*(4), 497-504.
[69]. Lee, I. (2019). The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. *Internet of things*, *7*, 100078.
[70]. Lee, S., Kim, Y., Kahng, H., Lee, S.-K., Chung, S., Cheong, T., Shin, K., Park, J., & Kim, S. B. (2020). Intelligent traffic control for autonomous vehicle systems based on machine learning. *Expert Systems with Applications*, *144*, 113074.
[71]. Li, M., Yin, D., Qiu, H., & Bai, B. (2022). Examining the effects of AI contactless services on customer psychological safety, perceived value, and hospitality service quality during the COVID-19 pandemic. *Journal of Hospitality Marketing & Management*, *31*(1), 24-48.
[72]. Li, X., Zhang, C., Li, X., & Zhang, W. (2023). Federated transfer learning in fault diagnosis under data privacy with target self-adaptation. *Journal of Manufacturing Systems*, *68*, 523-535.
[73]. Line, N. D., Dogru, T., El-Manstrly, D., Buoye, A., Malthouse, E., & Kandampully, J. (2020). Control, use and ownership of big data: A reciprocal view of customer big data value in the hospitality and tourism industry. *Tourism Management*, *80*, 104106.
[74]. López-Pintado, O., Dumas, M., García-Bañuelos, L., & Weber, I. (2019). Interpreted execution of business process models on blockchain. 2019 IEEE 23rd International Enterprise Distributed Object Computing Conference (EDOC),
[75]. Luo, J. M., Vu, H. Q., Li, G., & Law, R. (2021). Understanding service attributes of robot hotels: A sentiment analysis of customer online reviews. *International Journal of Hospitality Management*, *98*, 103032.
[76]. Maheswari, C., Priyanka, E., Thangavel, S., Vignesh, S. R., & Poongodi, C. (2020). Multiple regression analysis for the prediction of extraction efficiency in mining industry with industrial IoT. *Production Engineering*, *14*(4), 457-471.
[77]. Malik, V., Mittal, R., Mavaluru, D., Narapureddy, B. R., Goyal, S., Martin, R. J., Srinivasan, K., & Mittal, A. (2023). Building a secure platform for digital governance interoperability and data exchange using blockchain and deep learning-based frameworks. *Ieee Access*, *11*, 70110-70131.
[78]. Malola, A., & Maroun, W. (2019). The measurement and potential drivers of integrated report quality: Evidence from a pioneer in integrated reporting. *South African Journal of Accounting Research*, *33*(2), 114-144.
[79]. Manley, S. C., Hair Jr, J. F., Williams Jr, R. I., & McDowell, W. C. (2021). Essential new PLS-SEM analysis methods for your entrepreneurship analytical toolbox. *International Entrepreneurship and Management Journal*, *17*(4), 1805-1825.
[80]. Martin, N., Matt, C., Niebel, C., & Blind, K. (2019). How data protection regulation affects startup innovation. *Information systems frontiers*, *21*(6), 1307-1324.
[81]. Masud, R., & Md Sarwar Hossain, S. (2024). The Impact of Smart Materials And Fire-Resistant Structures On Safety In U.S. Public Infrastructure. *Journal of Sustainable Development and Policy*, *3*(03), 44-86. https://doi.org/10.63125/ygr1yk30

[82]. Md, K., & Sai Praveen, K. (2024). Hybrid Discrete-Event And Agent-Based Simulation Framework (H-DEABSF) For Dynamic Process Control In Smart Factories. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *4*(1), 72–96. https://doi.org/10.63125/wcqq7x08

[83]. Md Nahid, H., & Tahmina Akter Bhuya, M. (2024). An Empirical Study of Big Data–Enabled Predictive Analytics And Their Impact On Financial Forecasting And Market Decision-Making. *Review of Applied Science and Technology*, *3*(01), 143–182. https://doi.org/10.63125/1mjfqf10

[84]. Md Newaz, S., & Md Jahidul, I. (2024). AI-Powered Business Analytics For Smart Manufacturing And Supply Chain Resilience. *Review of Applied Science and Technology*, *3*(01), 183–220. https://doi.org/10.63125/va5gpg60

[85]. Md. Akbar, H. (2024). Computational Psychometrics and Digital Biomarker Modeling For Precision Mental Health Diagnostics. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 487–525. https://doi.org/10.63125/vg522x27

[86]. Md. Akbar, H., & Sharmin, A. (2022). Neurobiotechnology-Driven Regenerative Therapy Frameworks For Post-Traumatic Neural Recovery. *American Journal of Scholarly Research and Innovation*, *1*(02), 134–170. https://doi.org/10.63125/24s6kt66

[87]. Md. Foysal, H., & Subrato, S. (2022). Data-Driven Process Optimization in Automotive Manufacturing A Machine Learning Approach To Waste Reduction And Quality Improvement. *Journal of Sustainable Development and Policy*, *1*(02), 87-133. https://doi.org/10.63125/2hk0qd38

[88]. Md. Mosheur, R. (2025). AI-Driven Predictive Analytics Models For Enhancing Group Insurance Portfolio Performance And Risk Forecasting. *International Journal of Scientific Interdisciplinary Research*, *6*(2), 39–87. https://doi.org/10.63125/qh5qgk22

[89]. Md. Rabiul, K., & Khairul Alam, T. (2024). Impact Of IOT and Blockchain Integration On Real-Time Supply Chain Transparency. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 449–486. https://doi.org/10.63125/2yc6e230

[90]. Mengist, W., Soromessa, T., & Legese, G. (2020). Method for conducting systematic literature review and meta-analysis for environmental science research. *MethodsX*, *7*, 100777.

[91]. Mondal, S., Das, S., & Vrana, V. G. (2023). How to bell the cat? A theoretical review of generative artificial intelligence towards digital disruption in all walks of life. *Technologies*, *11*(2), 44.

[92]. Okazaki, S., Eisend, M., Plangger, K., de Ruyter, K., & Grewal, D. (2020). Understanding the strategic consequences of customer privacy concerns: A meta-analytic review. *Journal of Retailing*, *96*(4), 458-473.

[93]. Pan, X., Pan, X., Song, M., Ai, B., & Ming, Y. (2020). Blockchain technology and enterprise operational capabilities: An empirical test. *International journal of information management*, *52*, 101946.

[94]. Paraskevas, A. (2020). Cybersecurity in travel and tourism: a risk-based approach. In *Handbook of e-Tourism* (pp. 1-24). Springer.

[95]. Park, S. (2020). Multifaceted trust in tourism service robots. *Annals of Tourism Research*, *81*, 102888.

[96]. Pauli, T., Fielt, E., & Matzner, M. (2021). Digital industrial platforms. *Business & Information Systems Engineering*, *63*(2), 181-190.

[97]. Petersen, I.-h., & Kruss, G. (2021). Universities as change agents in resource-poor local settings: An empirically grounded typology of engagement models. *Technological Forecasting and Social Change*, *167*, 120693.

[98]. Pillai, S. G., Haldorai, K., Seo, W. S., & Kim, W. G. (2021). COVID-19 and hospitality 5.0: Redefining hospitality operations. *International Journal of Hospitality Management*, *94*, 102869.

[99]. Pluchinotta, I., Salvia, G., & Zimmermann, N. (2022). The importance of eliciting stakeholders' system boundary perceptions for problem structuring and decision-making. *European Journal of Operational Research*, *302*(1), 280-293.

[100]. Potter, R., O'Keeffe, V., Leka, S., Webber, M., & Dollard, M. (2019). Analytical review of the Australian policy context for work-related psychological health and psychosocial risks. *Safety science*, *111*, 37-48.

[101]. Prentice, C., Weaven, S., & Wong, I. A. (2020). Linking AI quality performance and customer engagement: The moderating effect of AI preference. *International Journal of Hospitality Management*, *90*, 102629.

[102]. Prybutok, V. R., & Sauser, B. (2022). Theoretical and practical applications of blockchain in healthcare information management. *Information & Management*, *59*(6), 103649.

[103]. Rahmadian, E., Feitosa, D., & Virantina, Y. (2023). Digital twins, big data governance, and sustainable tourism. *Ethics and Information Technology*, *25*(4), 61.

[104]. Ramírez-Montoya, M. S., Castillo-Martínez, I. M., Sanabria-Z, J., & Miranda, J. (2022). Complex thinking in the framework of education 4.0 and open innovation—a systematic literature review. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(1), 4.

[105]. Ranchordás, S., & Goanta, C. (2020). The new city regulators: Platform and public values in smart and sharing cities. *Computer law & security review*, *36*, 105375.

[106]. Rhodes, E., Scott, W. A., & Jaccard, M. (2021). Designing flexible regulations to mitigate climate change: A cross-country comparative policy analysis. *Energy policy*, *156*, 112419.

[107]. Riasanow, T., Jäntgen, L., Hermes, S., Böhm, M., & Krcmar, H. (2021). Core, intertwined, and ecosystem-specific clusters in platform ecosystems: analyzing similarities in the digital transformation of the automotive, blockchain, financial, insurance and IIoT industry. *Electronic markets*, *31*(1), 89-104.

[108]. Rifat, C., & Rebeka, S. (2023). The Role Of ERP-Integrated Decision Support Systems In Enhancing Efficiency And Coordination In Healthcare Logistics: A Quantitative Study. *International Journal of Scientific Interdisciplinary Research*, *4*(4), 265–285. https://doi.org/10.63125/c7srk144

[109]. Sabuj Kumar, S. (2023). Integrating Industrial Engineering and Petroleum Systems With Linear Programming Model For Fuel Efficiency And Downtime Reduction. *Journal of Sustainable Development and Policy*, *2*(04), 108-139. https://doi.org/10.63125/v7d6a941

[110]. Sabuj Kumar, S. (2024). Petroleum Storage Tank Design and Inspection Using Finite Element Analysis Model For Ensuring Safety Reliability And Sustainability. *Review of Applied Science and Technology*, *3*(04), 94–127. https://doi.org/10.63125/a18zw719

[111]. 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

[112]. Sai Praveen, K. (2024). AI-Enhanced Data Science Approaches For Optimizing User Engagement In U.S. Digital Marketing Campaigns. *Journal of Sustainable Development and Policy*, *3*(03), 01-43. https://doi.org/10.63125/65ebsn47

[113]. Semantha, F. H., Azam, S., Shanmugam, B., Yeo, K. C., & Beeravolu, A. R. (2021). A conceptual framework to ensure privacy in patient record management system. *Ieee Access*, *9*, 165667-165689.

[114]. Senyo, P. K., Liu, K., & Effah, J. (2019). Digital business ecosystem: Literature review and a framework for future research. *International journal of information management*, *47*, 52-64.

[115]. Seo, K. H., & Lee, J. H. (2021). The emergence of service robots at restaurants: Integrating trust, perceived risk, and satisfaction. *Sustainability*, *13*(8), 4431.

[116]. Shamim, S., Yang, Y., Zia, N. U., & Shah, M. H. (2021). Big data management capabilities in the hospitality sector: Service innovation and customer generated online quality ratings. *Computers in Human Behavior*, *121*, 106777.

[117]. Shams, R., Vrontis, D., Belyaeva, Z., Ferraris, A., & Czinkota, M. R. (2021). Strategic agility in international business: A conceptual framework for "agile" multinationals. *Journal of International Management*, *27*(1), 100737.

[118]. Shin, D. D. (2019). Blockchain: The emerging technology of digital trust. *Telematics and informatics*, *45*, 101278.

[119]. Shoflul Azam, T., & Md. Al Amin, K. (2024). Quantitative Study on Machine Learning-Based Industrial Engineering Approaches For Reducing System Downtime In U.S. Manufacturing Plants. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 526–558. https://doi.org/10.63125/kr9r1r90

[120]. Shukla, S., George, J. P., Tiwari, K., & Kureethara, J. V. (2022). Data security. In *Data ethics and challenges* (pp. 41-59). Springer.

[121]. Singh, S., & Aggarwal, Y. (2022). In search of a consensus definition of innovation: a qualitative synthesis of 208 definitions using grounded theory approach. *Innovation: The European Journal of Social Science Research*, *35*(2), 177-195.

[122]. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333-339.

[123]. Steenberg, J. W., Duinker, P. N., & Nitoslawski, S. A. (2019). Ecosystem-based management revisited: Updating the concepts for urban forests. *Landscape and urban planning*, *186*, 24-35.

[124]. Susanto, H., Fang Yie, L., Mohiddin, F., Rahman Setiawan, A. A., Haghi, P. K., & Setiana, D. (2021). Revealing social media phenomenon in time of COVID-19 pandemic for boosting start-up businesses through digital ecosystem. *Applied system innovation*, *4*(1), 6.

[125]. Taufick, R. D. (2021). The underdeterrence, underperformance response to privacy, data protection laws. *Technology in Society*, *67*, 101752.

[126]. Turetken, O., Dikici, A., Vanderfeesten, I., Rompen, T., & Demirors, O. (2020). The influence of using collapsed sub-processes and groups on the understandability of business process models. *Business & Information Systems Engineering*, *62*(2), 121-141.

[127]. Walsh, I., & Rowe, F. (2023). BIBGT: combining bibliometrics and grounded theory to conduct a literature review. *European Journal of Information Systems*, *32*(4), 653-674.

[128]. Wan, Y., Gao, Y., & Hu, Y. (2022). Blockchain application and collaborative innovation in the manufacturing industry: Based on the perspective of social trust. *Technological Forecasting and Social Change*, *177*, 121540.

[129]. Wang, G., Nixon, M., & Boudreaux, M. (2019). Toward cloud-assisted industrial IoT platform for large-scale continuous condition monitoring. *Proceedings of the IEEE*, *107*(6), 1193-1205.

[130]. Wang, J., Guo, B., Wang, X., & Lou, S. (2020). Closed or open platform? The nature of platform and a qualitative comparative analysis of the performance effect of platform openness. *Electronic Commerce Research and Applications*, *44*, 101007.

[131]. Wang, Z., Li, M., Lu, J., & Cheng, X. (2022). Business Innovation based on artificial intelligence and Blockchain technology. *Information Processing & Management*, *59*(1), 102759.

[132]. Wankmüller, C., & Reiner, G. (2020). Coordination, cooperation and collaboration in relief supply chain management. *Journal of Business Economics*, *90*(2), 239-276.

[133]. Waxin, M.-F., Knuteson, S. L., & Bartholomew, A. (2019). Drivers and challenges for implementing ISO 14001 environmental management systems in an emerging Gulf Arab country. *Environmental management*, *63*(4), 495-506.

[134]. Whaiduzzaman, M., Mahi, M. J. N., Barros, A., Khalil, M. I., Fidge, C., & Buyya, R. (2021). BFIM: Performance measurement of a blockchain based hierarchical tree layered fog-IoT microservice architecture. *Ieee Access*, *9*, 106655-106674.

[135]. Wiig, S., Aase, K., Billett, S., Canfield, C., Røise, O., Njå, O., Guise, V., Haraldseid-Driftland, C., Ree, E., & Anderson, J. E. (2020). Defining the boundaries and operational concepts of resilience in the resilience in healthcare research program. *BMC health services research*, *20*(1), 330.

[136]. Xu, X., Sun, G., Luo, L., Cao, H., Yu, H., & Vasilakos, A. V. (2021). Latency performance modeling and analysis for hyperledger fabric blockchain network. *Information Processing & Management*, *58*(1), 102436.
[137]. Xuelin, C., Yang, Z., Dongmei, Z., & Ruoyu, L. (2023). The evolution and knowledge change of innovation cooperation network in platform ecosystem: A computer simulation from complex network perspective. *Ieee Access*, *11*, 22221-22232.
[138]. Yrjölä, S., Matinmikko-Blue, M., & Ahokangas, P. (2023). Developing 6G visions with stakeholder analysis of 6G ecosystem. 2023 joint European conference on networks and communications & 6G summit (EuCNC/6G summit),
[139]. Zaheda, K. (2025a). AI-Driven Predictive Maintenance For Motor Drives In Smart Manufacturing A Scada-To-Edge Deployment Study. *American Journal of Interdisciplinary Studies*, *6*(1), 394-444. https://doi.org/10.63125/gc5x1886
[140]. Zaheda, K. (2025b). Hybrid Digital Twin and Monte Carlo Simulation For Reliability Of Electrified Manufacturing Lines With High Power Electronics. *International Journal of Scientific Interdisciplinary Research*, *6*(2), 143–194. https://doi.org/10.63125/db699z21
[141]. Zhang, B., Chu, Z., Cheng, L., & Zou, N. (2019). A quantitative safety regulation compliance level evaluation method. *Safety science*, *112*, 81-89.
[142]. Zhang, X., Feng, X., Jiang, Z., Gong, Q., & Wang, Y. (2023). A blockchain-enabled framework for reverse supply chain management of power batteries. *Journal of cleaner production*, *415*, 137823.
[143]. Zhao, D., & Wang, D. (2019). The research of tripartite collaborative governance on disorderly parking of shared bicycles based on the theory of planned behavior and motivation theories—A Case of Beijing, China. *Sustainability*, *11*(19), 5431.
[144]. Zhao, Y., Xu, X., & Wang, M. (2019). Predicting overall customer satisfaction: Big data evidence from hotel online textual reviews. *International Journal of Hospitality Management*, *76*, 111-121.
[145]. Zheng, R., Li, Z., & Na, S. (2022). How customer engagement in the live-streaming affects purchase intention and customer acquisition, E-tailer's perspective. *Journal of retailing and consumer services*, *68*, 103015.
[146]. Žigienė, G., Rybakovas, E., & Alzbutas, R. (2019). Artificial intelligence based commercial risk management framework for SMEs. *Sustainability*, *11*(16), 4501.
[147]. Zulqarnain, F. N. U. (2022). Policy Optimization for Sustainable Energy Security: Data-Driven Comparative Analysis Between The U.S. And South Asia. *American Journal of Interdisciplinary Studies*, *3*(04), 294-331. https://doi.org/10.63125/v4e4m413
[148]. Zulqarnain, F. N. U., & Subrato, S. (2021). Modeling Clean-Energy Governance Through Data-Intensive Computing And Smart Forecasting Systems. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 128–167. https://doi.org/10.63125/wnd6qs51
[149]. Zulqarnain, F. N. U., & Subrato, S. (2023). Intelligent Climate Risk Modeling For Robust Energy Resilience And National Security. *Journal of Sustainable Development and Policy*, *2*(04), 218-256. https://doi.org/10.63125/jmer2r39