

Research Article 03

Exploring Drivers Affecting Environmental Sustainability Reporting Practices: A Study Based on the Sri Lankan Hotel Industry

H.G.C. Senarathne¹, B.E.A. Jayasekara², L.M.F. Adams³

¹*Lincoln University College, Malaysia*

²*Department of Science for Technology, Faculty of Technology, University of Sri Jayewardenepura, Sri Lanka*

³*Institute of Knowledge Academia, Sri Lanka*

¹<https://orcid.org/0009-0008-4149-4218>

²<https://orcid.org/0009-0004-7433-5353>

Abstract

Sri Lankan SME hotels operate under increasing regulatory expectations across licensing, taxation, labour, health and safety, payment security, and personal data protection, yet many lack affordable, auditable systems to consistently demonstrate compliance. This paper reviews how modern technology enables compliance in Sri Lankan SME hotels and synthesises evidence from a systematic literature review using a PRISMA-inspired study selection process and thematic analysis of 58 included studies. The synthesis identifies six recurring findings. First, cloud-based property management and integrated platforms improve compliance readiness by standardising records, enabling traceability, and supporting consistent reporting. Second, security controls such as role-based access, logging, encryption, and backup practices are repeatedly linked with stronger data protection and incident resilience, which is increasingly relevant in light of emerging personal data protection requirements. Third, digital payments and automated reconciliation reduce control gaps and strengthen financial compliance through clearer audit trails. Fourth, digital checklists, e-forms, and workflow automation support routine operational compliance in areas such as hygiene, safety inspections, and staff governance. Fifth, technology-supported documentation and reporting improve external assurance, including licensing evidence and partner due diligence expectations. Sixth, adoption barriers in SME hotels remain significant, particularly cost sensitivity, skills constraints, unreliable connectivity, and weak governance routines, indicating the need for capability building and fit-for-purpose solution design. Overall, the review shows that compliance benefits are maximised when technology adoption is paired with simple governance practices, minimum security baselines, and staff training. The paper contributes a structured, evidence base to guide SME hotel operators, solution providers, and policymakers in prioritising technology investments that improve compliance outcomes while remaining practical for resource-constrained contexts such as Sri Lanka.

Keywords: Cloud computing, compliance, cyber security, digital governance, SME hotels

Corresponding Author: H.G.C. Senarathne – hgcsenarathne@gmail.com

Submitted: April 06, 2026; Revised: July 18, 2026; Accepted: August 02, 2026

Introduction

The hospitality sector in Sri Lanka plays a pivotal role in economic growth, foreign exchange earnings, and employment generation, with Small and Medium Enterprise (SME) hotels forming a substantial proportion of the industry (Sri Lanka Tourism Development Authority [SLTDA], 2023). These establishments, often family-owned or independently managed, provide unique, localized experiences that attract both domestic and international tourists (Ekanayake&Abeywardena, 2022). However, increasing regulatory requirements covering health and safety, taxation, environmental sustainability, and data privacy are present significant operational challenges. Concurrently, modern travelers demand greater transparency, hygiene assurance, and digital convenience (Sigala, 2020). Technology has emerged as a critical enabler for the hospitality sector globally, with innovations such as cloud-based systems, mobile applications, and data analytics reshaping operational models and compliance mechanisms (Buhalis & Leung, 2018). Despite these advancements, limited empirical research has examined how SME hotels in Sri Lanka can leverage such innovations to meet both regulatory standards.

Research Gap

While studies have explored technology adoption in the global hospitality sector, few have focused on how modern technology specifically supports compliance in SME hotels in emerging economies. The Sri Lankan context remains under-researched, particularly in integrating technology to address both regulatory compliance and evolving tourist expectations.

Research Objectives

- To examine the compliance requirements faced by SME hotels in Sri Lanka.
- To evaluate the role of modern technology in meeting these requirements.
- To synthesise technology-enabled mechanisms that improve compliance outcomes in Sri Lankan SME hotels.

Research Problem

The central research problem is the absence of practical, technology-enabled frameworks that help Sri Lankan SME hotels demonstrate and sustain regulatory compliance in a consistent and auditable manner.

Significance of the Study

Theoretical Significance - Extends Institutional Theory and the Technology–Organization–Environment (TOE) framework to compliance in SME hospitality in emerging markets.

Empirical Significance - Adds evidence from Sri Lanka, where SMEs dominate tourism but face systemic barriers to technological adoption (Fernando&Bandara, 2022).

Practical Significance - Provides guidance for policymakers, hospitality technology providers, and SME operators on implementing cost-effective, scalable, and sustainable compliance solutions.

Definition of Key Terms

Compliance - Adherence to statutory and regulatory requirements governing hotel operations.

Modern Technology - Digital tools and systems, including cloud computing, PMS, and mobile platforms, that support operational efficiency and compliance.

SME Hotels - As per SLTDA classifications, typically having fewer than 50 rooms and limited capital investment.

Literature Review

Compliance as a Multidimensional Management Task

The reviewed literature suggests that compliance in SME hotels is best understood as a multidimensional management task rather than a narrow question of legal conformity alone. In operational terms, hotels must maintain a continuing level of alignment across licensing requirements, tax and financial reporting, labour administration, health and safety practices, sanitation routines, payment security, environmental responsibilities, and personal data handling. Larger hotel groups often manage these obligations through specialist departments and formal reporting structures, but Sri Lankan SME hotels frequently rely on owners, front office supervisors, or a small management team to coordinate all these activities at once. This organisational reality is important because it means that compliance is often not weak due to indifference. Instead, it becomes weak when record keeping is fragmented, responsibilities are not clearly assigned, or evidence cannot be retrieved quickly when regulators, partners, or guests expect proof of good practice (Gajjar & Parmar, 2021; Perera & Weerasinghe, 2021).

This broader understanding also helps explain why compliance and performance cannot be cleanly separated in hospitality settings. When billing records are inconsistent, guest registration data are incomplete, hygiene logs are missing, or safety checks are undocumented, the effect is not only regulatory exposure. The hotel may also face slower service, disputes with guests, difficulty handling refunds, weak internal control, and reputational loss on digital platforms. In this sense, compliance is embedded in the operational quality of the hotel itself. The literature increasingly supports this view by treating compliance as part of service reliability, information quality, and managerial discipline rather than a purely external burden imposed by regulators (Buhalis & Leung, 2018; Ali et al., 2023).

For Sri Lankan SME hotels, the multidimensional nature of compliance is especially significant because the sector is highly heterogeneous. Small beach hotels, boutique city properties, transit-oriented lodgings, and family-operated guest accommodation may all face a common demand for safe, reliable, and auditable operations, yet their internal capacity differs greatly. A one-size-fits-all compliance model is therefore unrealistic. What remains common across property types, however, is the central need for structured information. When a hotel can reliably capture, store, retrieve, and review operational data, it becomes better able to demonstrate adherence to expected standards. This is why the literature repeatedly points to technology as an enabling infrastructure for compliance rather than a simple efficiency tool (Law et al., 2018; Mariani & Borghi, 2021).

Another important insight from the reviewed studies is that compliance must be seen in both internal and external terms. Internal compliance includes adherence to the hotel's own rules, approval processes, security routines, and record retention practices. External compliance refers to laws, inspections, industry standards, and partner expectations. These two spheres are closely linked. A hotel that lacks internal control discipline is unlikely to present strong external compliance readiness. Technology helps close this gap by formalising internal routines. Required fields, role-based permissions, digital logs, time-stamped task completion, and automatic reporting all create conditions in which internal discipline is easier to maintain and external evidence becomes easier to produce. This strengthens the argument that technology adoption in SME hospitality should be evaluated not only through productivity outcomes but also through its capacity to reduce control gaps and support consistent compliance behaviour.

The literature also indicates that compliance is increasingly shaped by the digital behaviour of guests and commercial partners. Guests expect secure payments, accurate confirmations, visible professionalism, and fast issue resolution. Online travel platforms and payment providers increasingly expect clean records, timely reconciliations, and documented handling of operational issues. These expectations are not always framed in legal language, yet they raise the effective compliance threshold for hotels. A property that cannot demonstrate control over guest data, refunds, billing, or safety routines may struggle commercially even before formal regulatory sanctions occur. This means that compliance in SME hotels is no longer only about avoiding penalties. It is part of how trust is built and sustained in the contemporary tourism market (Sigala, 2020; Wang et al., 2022).

Technology as an Evidence-Producing Infrastructure

A major pattern across the literature is that technology improves compliance not merely by speeding up work but by making activities evidential. This point matters for SME hotels because many compliance failures emerge at the moment evidence is requested rather than at the moment the underlying task is performed. A room may have been cleaned, a maintenance check may have been completed, a guest complaint may have been resolved, or a payment may have been received correctly, yet if these actions are not recorded in a consistent and retrievable way, the hotel remains exposed. Cloud-based systems, integrated property management platforms, digital forms, and workflow applications reduce this exposure by turning daily operational actions into data that can be verified later (Law et al., 2018; Ali et al., 2023).

Property management systems occupy a central place in this process because they link reservations, front office operations, billing, housekeeping status, and reporting within a single environment. For compliance purposes, their value lies not only in convenience but in standardisation. Standardised fields reduce ambiguity in records. Centralised databases reduce duplication. Automated timestamps improve traceability. User-level permissions make accountability more visible. These capabilities are especially useful in SME hotels where the same staff member may carry out several roles across the guest journey. In manual environments, multitasking often leads to undocumented exceptions and missing records. In digital environments, the system can retain critical information even when individual staff members change or forget the details of an event (Buhalis & Leung, 2018).

Evidence-producing infrastructure is also increasingly relevant in relation to data protection and security compliance. Hotels collect names, contact details, identification documents, payment information, and behavioural data from guests and partners. As this information grows more valuable and more sensitive, the need for controlled access, logging, retention

discipline, and recovery capability becomes more important. The literature on privacy, smart tourism, and cyber risk indicates that hotels require not only technical tools but also a simple control architecture that makes information handling auditable over time (Gong & Schroeder, 2022; Karadayi Usta, 2024). In practice, this means that technology supports compliance most effectively when it is configured to generate evidence of who accessed data, what was changed, when backups were made, and how incidents were handled.

A related benefit concerns payment and financial control. Digital payment integration, automated reconciliation, and exception visibility help reduce the weakness of fragmented cash handling and delayed financial reporting. In smaller hotels, manual reconciliation often depends on a few trusted individuals and may be vulnerable to oversight gaps, unrecorded adjustments, or delayed detection of discrepancies. Where payment activity is linked to operational records and audit logs, control becomes stronger because the evidence chain is clearer. This aligns with the literature that treats payment security standards and internal reporting discipline as mutually reinforcing rather than separate domains (Payment Card Industry Security Standards Council, 2022; PCI Security Standards Council, 2024).

The reviewed studies also show that evidence-producing technology extends beyond the front office and back office into daily compliance routines. Mobile checklists, e-forms, digital inspections, and maintenance workflows are effective because they shorten the distance between action and documentation. In hygiene, food safety, maintenance, and staff governance tasks, delayed documentation weakens compliance credibility. When staff can complete a checklist on the spot, attach a note or image, and create a time-stamped record, the hotel builds a stronger compliance history with minimal extra administrative burden. This is especially valuable in SME environments where supervision capacity is limited. A digital workflow can function as a light form of governance by making completion visible, overdue items obvious, and follow-up actions easier to assign and review (Gajjar & Parmar, 2021; Law et al., 2018).

However, the literature also warns that evidence-producing infrastructure only works when governance routines are aligned with it. If hotels continue to rely on informal verbal approval, shared passwords, duplicated offline records, or inconsistent data entry, then even technically capable systems may fail to deliver compliance value. Technology therefore needs to be embedded within a minimum viable governance model that defines who is responsible for key compliance tasks, which records must be retained, how exceptions are reviewed, and what basic security practices are expected. This interaction between digital systems and governance routines is central to the paper's argument because it explains why technology can dramatically improve compliance readiness in some SME hotels while producing only modest gains in others (ISO, 2021; National Institute of Standards and Technology, 2024).

Operational Domains where Compliance Technology Matters Most

The literature reviewed in this study indicates that the benefits of technology-enabled compliance are not evenly distributed across all hotel functions. Some domains show especially strong potential for improvement because they are document-intensive, repetitive, and vulnerable to inconsistency under manual administration. One of the clearest domains is guest registration and identity-related documentation. Front office processes require accuracy because they influence room allocation, payment responsibility, guest communication, and legal record retention. Errors at this stage can affect financial reporting, dispute handling, and security. Digital registration workflows support greater consistency by reducing illegible handwriting, incomplete fields, and lost records. They also support easier

retrieval during inspections or internal review, which is critical for properties that operate with lean staffing structures.

A second domain is hygiene, housekeeping, and routine operational safety. Cleanliness has become both a service expectation and a compliance concern, especially since the pandemic intensified guest awareness of sanitation standards. Yet manual housekeeping logs or paper checklists can be incomplete, delayed, or difficult to verify. Digital checklists improve this situation because they can assign responsibility, record completion time, escalate unresolved items, and retain evidence in a central location. In small hotels, where a manager may not physically inspect every room or common area, these tools provide a practical layer of oversight without requiring heavy bureaucracy. This makes them especially suitable for SME environments that need discipline but cannot support large compliance departments (Sigala, 2020; Gajjar&Parmar, 2021).

A third domain concerns maintenance and asset-related compliance. Many compliance failures in hotels are linked not to major strategic weakness but to small operational lapses such as delayed repairs, overlooked safety faults, broken controls, or absent documentation of preventive maintenance. Technology can improve this area through maintenance tickets, scheduled task reminders, digital sign-off, and simple escalation logic. The value is twofold. First, it improves the physical reliability of the property, which matters directly for guest experience. Second, it creates evidence that management is monitoring and responding to operational risks. In the absence of such evidence, hotels may struggle to demonstrate due diligence when incidents or disputes arise.

Financial and tax-related processes constitute another crucial compliance domain. SME hotels often operate under significant cash flow pressure and may use a mix of cash, card, transfer, and platform-mediated payments. Without integrated systems, reconciliation becomes labour-intensive and vulnerable to mismatch. Delayed or inaccurate reconciliation can weaken financial control, complicate taxation, and undermine confidence in reported figures. The literature consistently suggests that digital payment integration, exception visibility, and time-stamped transaction records improve not only finance accuracy but also wider compliance readiness. This is because financial transparency supports more reliable reporting, stronger accountability, and quicker response when anomalies occur (Payment Card Industry Security Standards Council, 2022; PCI Security Standards Council, 2024).

Human resource and staff governance functions also deserve greater attention in the compliance discussion. In many SME hotels, labour administration is still relatively informal, with rostering, attendance, approvals, and training evidence managed through basic manual tools. While this may appear manageable in small teams, it becomes problematic when disputes, inspections, or high turnover create the need for reliable records. Digital attendance, shift logging, acknowledgement records, and training confirmation tools can strengthen internal governance without requiring complex human resource platforms. Given the seasonal and labour-intensive nature of hospitality work, these functions can materially improve both compliance and managerial control.

Finally, data protection has emerged as a cross-cutting domain that affects nearly every hotel process. Guest profiles, billing details, contact information, payment interactions, and communication histories all generate data that must be handled responsibly. The literature suggests that effective compliance in this area depends less on abstract privacy statements and more on simple operational controls: role-based access, secure credentials, backup routines, incident logging, and clear responsibility for data handling. For Sri Lankan SME hotels, the practical challenge is to translate emerging legal and market expectations into a

manageable daily discipline. Technology provides the tools for this, but the hotel must still make deliberate choices about configuration, access, retention, and review (Parliament of Sri Lanka, 2022; Data Protection Authority of Sri Lanka, 2024; Gong & Schroeder, 2022).

Why Adoption Remains Uneven in Sri Lankan SME Hotels

Despite the strong compliance rationale for digital adoption, the literature indicates that uptake remains uneven across Sri Lankan SME hotels. Cost sensitivity remains a major reason. Even when cloud systems reduce capital expenditure compared with on-premises solutions, hotels still face subscription commitments, implementation fees, training time, possible device purchases, and the opportunity cost of changing familiar routines. For small operators recovering from demand shocks or working with thin margins, these costs can appear risky. This helps explain why technology is sometimes adopted in a piecemeal way rather than as part of a deliberate compliance strategy. The hotel may digitise bookings but not reconciliation, or use a PMS without activating access controls, backups, or structured reporting features. Partial adoption can produce limited efficiency gains while leaving major compliance gaps unresolved (Fernando & Bandara, 2022).

Digital literacy is another persistent barrier. Hospitality staff may be highly experienced in customer interaction but less confident in data entry discipline, control settings, dashboard interpretation, or security practice. Owners may similarly be unsure how to assess vendors, configure systems, or identify which features matter most for compliance. This creates a risk of both over-buying and under-using technology. Some hotels purchase systems with more complexity than they can manage, leading to frustration and workarounds. Others choose low cost tools that do not adequately support reporting, auditability, or data protection. In both cases, the central problem is not the absence of technology in the market, but the absence of fit between system design, staff capability, and organisational need (Nikopoulou et al., 2023; Santarsiero et al., 2024).

Infrastructure conditions also shape uneven adoption. Cloud-based and connected systems depend on stable internet access, electricity continuity, and dependable device availability. These conditions vary across tourism locations. In practice, hotels that experience regular connectivity problems may lose trust in real-time systems and fall back on paper-based or offline workarounds. Once parallel systems emerge, compliance integrity is weakened because the evidence base becomes fragmented. This is particularly problematic in inspection, payment, and data handling contexts where consistency of records is essential. The literature therefore suggests that fit-for-purpose implementation in emerging market settings must account for infrastructure variability rather than assume the operating environment of larger urban chains (Nyamwesa, 2024).

Organisational culture also matters more than it first appears. Many SME hotels rely on informal decision-making and owner-centric control. In such settings, documentation may be seen as secondary to practical experience or personal supervision. While this approach may work when the property is very small and stable, it becomes fragile as guest volumes increase, staff rotate, and compliance expectations tighten. Technology introduces structure, visibility, and consistency, but it may also be perceived as reducing flexibility or exposing hidden weaknesses. Staff resistance can emerge if systems are framed as surveillance rather than support. The reviewed studies imply that successful adoption depends on communication, involvement, and a clear explanation of why the technology is being introduced and how it reduces risk for the business as a whole (Boto García, 2023; Nikopoulou et al., 2023).

Another reason for uneven adoption is weak governance design at the implementation stage. Hotels may install a system but fail to define who owns user administration, who checks backups, who reviews exception reports, or how digital checklists should be monitored. Without these routines, the hotel has technology but not a compliance process. This distinction is important because it explains why some SMEs report low benefit even after acquiring modern systems. The literature strongly indicates that light governance is better than no governance. A simple monthly review, basic role definitions, documented minimum controls, and a small set of key reports can materially improve outcomes without creating excessive burden (ISO, 2021; National Institute of Standards and Technology, 2024).

The Sri Lankan context sharpens all of these issues because hotels have had to navigate recovery pressures, changing traveller behaviour, and tighter expectations regarding payment, privacy, and operational reliability at the same time. In this environment, compliance may appear to compete with survival. Yet the reviewed evidence suggests the opposite. Hotels that lack structured systems often spend more time correcting avoidable errors, defending disputes, and recreating missing evidence. Technology adoption therefore becomes uneven not because it lacks value, but because the route to value is not always clear, affordable, or supported. This points directly to the need for context-sensitive implementation models and stronger capability support across the SME segment (SLTDA, 2023; World Economic Forum, 2024).

Understanding Compliance in SME Hotels

Compliance in the hospitality sector involves adherence to legal, operational, environmental, safety, and data privacy regulations (Gajjar & Parmar, 2021). While global literature positions compliance as both a legal obligation and a driver of operational excellence (Jones et al., 2016), much of this research focuses on large-scale hotels with dedicated compliance departments. In contrast, SME hotels, particularly in emerging economies like Sri Lanka are often face unique constraints, including limited human resources, informal management practices, and insufficient technological infrastructure (Perera & Weerasinghe, 2021).

Some scholars suggest that SME compliance is largely reactive, triggered by regulatory audits or penalties (Fernando & Bandara, 2022), while others highlight market-driven compliance motivated by guest expectations for safety and ethical operations (DiMaggio & Powell, 1983). This duality is seldom addressed in Sri Lankan literature, where inconsistent regulatory enforcement further complicates compliance. Moreover, fragmented manual systems can lead to errors, missing documentation, and reputational risks. Addressing this requires context specific strategies, particularly affordable, technology-enabled frameworks that reduce administrative burdens while enhancing service quality.

Modern Technology in Hospitality

Technological innovation has transformed hospitality operations globally, reshaping service delivery, guest engagement, and compliance processes (Buhalis & Leung, 2018). Cloud-based Property Management Systems (PMS), integrated Point of Sale (POS) solutions, digital audit tools, and mobile guest apps streamline reporting, automate recordkeeping, and reduce operational errors (Ali et al., 2023). However, much of the literature showcases implementations in resource-rich environments, often in large hotel chains, raising questions about scalability for SMEs in developing contexts (Mariani & Borghi, 2021).

While global adoption trends highlight the benefits of AI, IoT, and big data for compliance monitoring (Law et al., 2018), Sri Lankan SMEs face barriers such as high initial

investment, limited digital literacy, and uncertainty about measurable returns (Fernando & Bandara, 2022). Furthermore, studies rarely address integration challenges, system downtime risks, or cybersecurity vulnerabilities in smaller operations. This suggests a research gap in understanding how modern technology can be adapted for cost-sensitive, resource-limited SME hotels while ensuring compliance resilience.

However, sustainability-focused tourists now demand verifiable evidence of eco-friendly practices, pressuring hotels to track and report environmental compliance (UNWTO, 2022). Literature from developed economies provides frameworks for integrating guest experience and compliance reporting, but there is limited empirical work examining how SMEs in Sri Lanka can achieve both without straining operational capacity. This creates a knowledge gap at the intersection of customer satisfaction, compliance, and technological adaptation.

Intersection of Compliance and Technology

Modern technology increasingly functions as a compliance enabler, automating documentation, ensuring secure recordkeeping, and facilitating audit readiness (Law et al., 2018). Cloud-based PMS platforms can centralize guest data, automatically generate tax reports, and track safety inspections, while IoT solutions can monitor environmental performance in real time (Jones et al., 2016). Yet, many studies overlook the socio-technical challenges SMEs face, including staff resistance, inadequate training, and partial technology adoption that fails to fully address compliance needs (Ali et al., 2023).

Recent literature emphasises that compliance in digitally enabled hotels is shaped by four interacting layers: regulatory obligations (for example, data protection and sector licensing), industry standards (such as PCI DSS for payment environments), information security management controls (for example, ISO/IEC 27001), and operational risk intelligence informed by contemporary threat landscapes. This framing helps explain why cloud governance features such as encryption, access control, segmentation, incident logging, and automated evidence collection are increasingly treated as core compliance capabilities rather than optional IT enhancements (Gong & Schroeder, 2022; Karadayi-Usta, 2024; PCI Security Standards Council, 2024; ISO, 2022; European Union Agency for Cybersecurity, 2023).

Moreover, while technology promises efficiency, it also introduces new compliance risks, such as data breaches, non-conformance to digital privacy regulations, and over-reliance on third-party vendors. Research from developed contexts often assumes robust internet infrastructure and regulatory clarity—conditions that are not always present in Sri Lanka. This highlights the necessity for tailored implementation models that consider local infrastructure, skills availability, and enforcement realities.

The Sri Lankan Context

Sri Lanka's tourism sector is recovering from a combination of economic crisis, political instability, and the COVID-19 pandemic, with SMEs at the forefront of revitalization efforts (SLTDA, 2023). Unlike large hotels with structured compliance frameworks, SMEs often rely on owners or minimal staff for regulatory matters, leading to fragmented processes and ad-hoc responses to compliance requirements (Perera & Weerasinghe, 2021). While internet access and the affordability of cloud solutions have improved, adoption remains hindered by capital constraints, lack of digital training programs, and minimal government incentives for technology uptake (Fernando & Bandara, 2022).

From a compliance perspective, SME hotels now operate under a tightening mix of legal, regulatory and market expectations. Key pressures include the Personal Data Protection Act (No. 9 of 2022) and related guidance issued by Sri Lanka's Data Protection Authority, sector registration and inspection requirements administered by the Sri Lanka Tourism Development Authority, and payment security expectations aligned to PCI DSS for card transactions. In practice, this pushes hotels towards cloud based systems that can evidence controls through audit trails, role based access, logging, and automated retention, and towards recognised security and compliance frameworks such as ISO/IEC 27001:2022 and the NIST Cybersecurity Framework 2.0. (Parliament of Sri Lanka, 2022; Data Protection Authority, 2024; Sri Lanka Tourism Development Authority, 2024; PCI Security Standards Council, 2024; ISO, 2022; NIST, 2024).

Literature on Sri Lanka's hospitality sector often focuses on marketing, service quality, and operational challenges, with comparatively little attention given to technology-enabled compliance. Furthermore, there is limited discussion of how safety and sustainability are reshaping compliance priorities for SMEs. This represents a substantial research gap, reinforcing the need for an integrated examination of technology and compliance within the Sri Lankan SME hotel context.

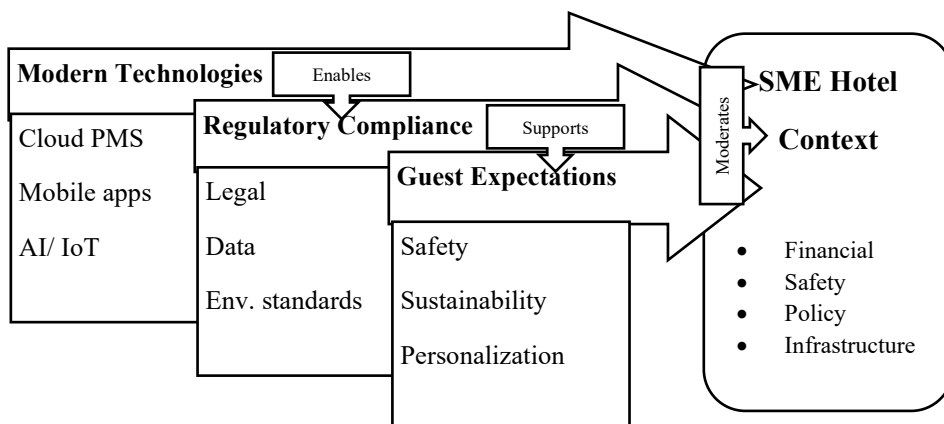


Figure 1: Conceptual Framework for Technology-enabled Compliance in Sri Lankan SME Hotels

Source: Authors' compilation based on previous literature

Modern technology (e.g., cloud PMS, mobile applications, and digital audit tools) enables regulatory compliance, which in turn supports SME hotels in meeting evolving tourist expectations (Buhalis & Leung, 2018; Ali et al., 2023; Sigala, 2020). The Sri Lankan SME hotel context moderates this relationship, influencing the effectiveness of technology adoption (Fernando & Bandara, 2022; Perera & Weerasinghe, 2021). The framework draws on Institutional Theory (DiMaggio & Powell, 1983) and the Technology–Organization–Environment (TOE) framework.

Research Methodology

This study adopted a systematic literature review design to identify, evaluate, and synthesise evidence concerning the role of cloud computing solutions in supporting compliance among SME hotels in Sri Lanka. The review process was guided by the PRISMA 2020 framework to support transparent reporting of literature identification, screening, eligibility assessment, and final source selection (Page et al., 2021). A systematic literature review was considered appropriate because it enables a structured synthesis of fragmented evidence across hospitality technology, regulatory compliance, SME digital adoption, and emerging market contexts (Snyder, 2019).

Following the literature selection process, thematic synthesis was used to analyse and integrate findings from the included sources. Thematic synthesis enables researchers to code findings, develop descriptive themes, and generate broader analytical interpretations across conceptually and methodologically diverse literature (Thomas & Harden, 2008). This approach was suitable because the evidence base included empirical studies, conceptual publications, industry standards, policy documents, legislation, and official reports.

Due to substantial differences in research designs, geographic settings, compliance measures, technological applications, and reported outcomes across the included sources, statistical meta-analysis was not appropriate. The evidence was therefore synthesised qualitatively to identify recurring compliance mechanisms, implementation barriers, enabling conditions, and contextual implications relevant to Sri Lankan SME hotels.

The PRISMA 2020 framework provides guidance for transparently reporting why a review was conducted, how evidence was identified and selected, and what sources were eventually included. Thematic synthesis supports the development of descriptive and analytical themes from findings across multiple studies.

Search Strategy

A structured literature search was conducted between May and July 2025 using Scopus, Web of Science, ScienceDirect, Emerald Insight, and Google Scholar. These sources were selected to capture multidisciplinary literature across hospitality management, tourism, information systems, regulatory compliance, cybersecurity, and SME digital transformation. The search strategy was developed by grouping terms into three principal concepts such as SME hospitality businesses, compliance requirements, and digital or cloud-based technologies. Boolean operators, phrase searching, truncation, and database-specific search functions were applied where supported. The principal search string was structured as follows.

("SME hotel*" OR "small hotel*" OR "small and medium hotel*" OR "independent hotel*" OR "hospitality SME*") AND (compliance OR regulation* OR governance OR audit* OR licensing OR taxation OR safety OR cybersecurity OR "data protection" OR "payment security") AND ("cloud computing" OR "cloud based system*" OR "property management system*" OR PMS OR "digital transformation" OR "hospitality technology" OR "mobile application*" OR "digital workflow*" OR "digital audit*")

A supplementary contextual search was conducted by combining the principal concepts with the following geographic terms:

("Sri Lanka" OR "South Asia" OR "emerging econom*" OR "developing countr*")

The geographic terms were not made compulsory in every database search because doing so could have excluded relevant evidence from comparable emerging economy and international hospitality contexts. Instead, Sri Lankan studies were prioritised during screening, while studies from other settings were retained when they offered applicable evidence concerning SME hotels, cloud technologies, regulatory compliance, cybersecurity, payment controls, or digital governance.

The search process and source selection were documented in accordance with the reporting principles of PRISMA 2020 and PRISMA S, which emphasise transparent reporting of databases, search dates, search terms, limits, and record management procedures (Page et al., 2021; Rethlefsen et al., 2021).

Inclusion and Exclusion Criteria

Only peer-reviewed journal articles, conference papers, and official industry reports published between 2010 and 2025 were included to ensure relevance to current technological and regulatory contexts. Sources had to address at least one of the following.

- Compliance in the hospitality sector.
- Technology adoption in hospitality or SMEs.
- Evolving tourist expectations.
- Sri Lankan or comparable emerging market contexts.

Non-English publications, opinion pieces without empirical or theoretical grounding, and sources unrelated to the hospitality industry were excluded.

Data Extraction and Analysis

The selected sources were reviewed in full, and relevant information was recorded in a structured matrix covering authorship, year, source type, geographic context, methodology, technological focus, compliance area, key findings, and relevance to Sri Lankan SME hotels.

The evidence was analysed using thematic synthesis following Thomas and Harden (2008). Five broad categories initially guided the review. Through coding, comparison, and refinement, these categories developed into six final themes presented in the Findings section. Due to differences in methods, settings, and reported outcomes, statistical meta-analysis was not appropriate, and the evidence was synthesised qualitatively.

Data Sources and Selection Process

The search identified 450 records. After removing 60 duplicates, 390 records were screened by title and abstract. A total of 280 records were excluded because they did not meet the review criteria. The full texts of 110 sources were assessed for eligibility, of which 52 were excluded. Finally, 58 sources met the inclusion criteria and were included in the thematic synthesis. The selection process was reported using a PRISMA-inspired flow diagram (Page et al., 2021).

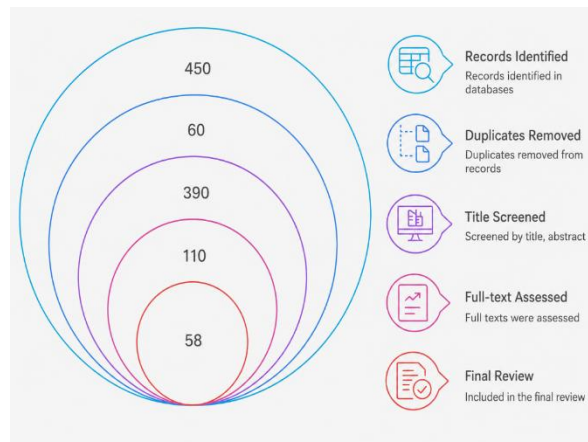


Figure 2: Literature Selection Flow Diagram

This PRISMA (Page et al., 2021) inspired flow diagram outlines the process of identifying, screening, and selecting literature for inclusion in the review. It documents the initial database search results, the removal of duplicates, the screening of titles and abstracts, full-text eligibility assessments, and the final inclusion of 58 studies in the thematic analysis.

Results and Interpretations

This section summarises results from 58 studies. Using thematic analysis, it identifies six technology enabled compliance pathways relevant to Sri Lankan SME hotels. Evidence shows compliance improves most when technology supports standardised records, traceable audit trails, and repeatable governance routines, rather than manual, ad hoc practices.

Overview of the Evidence Base

The 58 studies include conceptual, empirical, standards, and policy sources on hospitality compliance and technology. They show compliance is multi-dimensional, spanning licensing and reporting, financial controls and payment security, labour and safety, plus data protection and cyber resilience. Technology helps SMEs evidence compliance through reliable records, logs, and consistent workflows as digital traceability expectations rise (Buhalis & Leung, 2018; Gajjar & Parmar, 2021; Law et al., 2018).

Theme 1 - Standardisation and Auditability through Cloud-based Platforms

Across the reviewed studies, cloud-based PMS and integrated hospitality platforms strengthen compliance by standardising records and generating audit-ready evidence such as time-stamped entries, access logs, and consistent reports for inspections and partner checks (Ali et al., 2023; Buhalis & Leung, 2018; Law et al., 2018).

Theme 2 - Personal Data Protection and Security Baselines as Compliance Drivers

Evidence shows data protection and cyber security are now central to hotel compliance. SME hotels benefit most from baseline controls such as role-based access, encryption,

backups, patching, and a simple incident response plan aligned with recognised frameworks. This is increasingly important in Sri Lanka under emerging personal data protection expectations (ISO, 2022; National Institute of Standards and Technology, 2024; Parliament of Sri Lanka, 2022; Data Protection Authority of Sri Lanka, 2024).

Theme 3 - Payment Security and Financial Compliance through Digital Controls

Financial compliance improves when digital payments and reconciliation are integrated into operational systems, creating clear audit trails, visible exceptions, and reduced cash handling risk. Where card data is involved, alignment with PCI DSS expectations supports stronger control discipline (Payment Card Industry Security Standards Council, 2022; PCI Security Standards Council, 2024).

Theme 4 - Operational Compliance via Workflow Automation and Digital Checklists

Operational compliance becomes more reliable when routine checks are digitised through workflows, mobile forms, and checklists that can be assigned, time-stamped, tracked, and reviewed, which helps SMEs manage hygiene, safety, maintenance, and staff governance with limited supervision (Gajjar & Parmar, 2021; Law et al., 2018).

Theme 5 - Evidence Readiness for Licensing, Inspections, and Partner due Diligence

Technology also improves evidence readiness. Centralised and retrievable records allow SME hotels to respond faster to licensing and inspection requests, and to meet due diligence expectations from platforms and business partners without scrambling to rebuild paperwork (Ali et al., 2023; Buhalis & Leung, 2018).

Theme 6 - Adoption Barriers and Enabling Conditions in the Sri Lankan SME Context

Finally, compliance gains depend on adoption conditions. Cost constraints, skills gaps, connectivity issues, and weak governance routines can limit impact, so benefits are highest when implementation includes basic roles, simple policies, staff training, and periodic internal reviews (Ekanayake&Abeywardena, 2022; Fernando&Bandara, 2022; International Organization for Standardization, 2021).

Discussion

Technology-enabled compliance in SME hotels is most effective when it converts compliance from ad hoc effort into a standardised, evidence-based routine. Across the 58 studies, the strongest benefits occur when systems improve traceability, strengthen internal controls, and reduce dependence on individual staff behaviour. However, technology alone is not enough. Compliance outcomes improve when adoption is supported by basic governance, minimum security baselines, and staff capability building (International Organization for Standardization, 2021; Law et al., 2018).

Theme 1 shows cloud-based PMS adoption can shift SMEs from reactive compliance to routine evidence generation through consistent records and logs (Ali et al., 2023; Buhalis & Leung, 2018; Law et al., 2018).

Theme 2 highlights that SMEs gain more from practical security basics than complex programmes, including role-based access, encryption, backups, patching, and a simple incident response plan aligned with recognised frameworks and Sri Lankan data protection expectations (ISO, 2022; National Institute of Standards and Technology, 2024; Parliament of Sri Lanka, 2022; Data Protection Authority of Sri Lanka, 2024).

Theme 3 indicates integrated digital payments and reconciliation improve financial transparency, reduce cash exposure, and strengthen audit readiness (Payment Card Industry Security Standards Council, 2022; PCI Security Standards Council, 2024).

Theme 4 shows workflow tools embed daily compliance by making completion visible and reviewable across hygiene, safety, maintenance, and staff duties (Gajjar & Parmar, 2021; Law et al., 2018).

Theme 5 finds centralised documentation reduces time and errors when demonstrating compliance to regulators and partners (Ali et al., 2023; Buhalis & Leung, 2018).

Theme 6 reinforces that sustained compliance requires light governance routines and capability building, especially in settings with skills gaps and staff turnover (Ekanayake&Abeywardena, 2022; Fernando&Bandara, 2022; International Organization for Standardization, 2021).

Overall, the literature supports a minimum viable compliance model for Sri Lankan SME hotels: standardise records through core systems, apply baseline security, integrate payment controls, digitise routine workflows, and maintain a simple cadence of review and accountability. Future research can test which combinations deliver the greatest gains under resource constraints (International Organization for Standardization, 2021; National Institute of Standards and Technology, 2024).

Expanded Discussion of Strategic Implications

The findings of this review indicate that technology-enabled compliance should be interpreted as a strategic capability for Sri Lankan SME hotels rather than an isolated administrative improvement. The strategic value arises because compliance now intersects directly with guest trust, partner expectations, payment assurance, reputational resilience, and business continuity. In digital tourism markets, many aspects of compliance are externally visible even when the legal rules themselves are not. Guests notice confirmation accuracy, secure payment handling, professional communication, hygiene consistency, and the speed with which issues are resolved. Commercial partners notice whether documentation is complete, transactions are traceable, and obligations can be evidenced without delay. These signals influence market credibility, which means compliance capability increasingly affects competitiveness as well as legal safety (Sigala, 2020; Wang et al., 2022).

One strategic implication is that compliance can no longer be treated as something separate from service design. Contactless processes, digital confirmations, accurate invoicing, visible

response records, and properly managed guest data all support convenience while also strengthening control. The same technology feature can therefore satisfy both market demand and compliance needs. This dual value is especially important for SME hotels because they must often justify every investment against immediate operating pressures. A compliance-oriented technology investment becomes easier to defend when it also improves guest experience, staff coordination, or revenue visibility. The literature suggests that this combined value proposition is one of the strongest reasons cloud-based and integrated systems have become more relevant in hospitality contexts (Buhalis & Leung, 2018; Ali et al., 2023).

Another strategic implication concerns resilience. Hotels operate in an environment shaped by demand shocks, security incidents, staff turnover, and increasing data dependence. Under such conditions, manual and person-dependent compliance models are fragile. A well-configured digital environment supports resilience by preserving records, maintaining continuity of information, and making recovery easier after disruption. Backups, user logs, incident checklists, and centralised records are not only technical controls. They are organisational stabilisers. For small hotels that lack deep management layers, this stabilising effect is highly valuable because it reduces dependence on individual memory and informal verbal coordination. The literature on cyber risk and digital maturity reinforces this point by showing that minimum security baselines and documented routines often matter more for resilience than advanced technical sophistication (ISO, 2022; National Institute of Standards and Technology, 2024; Karadayi Usta, 2024).

The review also highlights a strategic tension. Technology can improve compliance only when it is aligned with the real operating model of the hotel. Systems that are too complex, too generic, or weakly supported may increase frustration and lead to shadow processes outside the official workflow. This is why the concept of fit-for-purpose technology is central. Sri Lankan SME hotels need solutions that are auditable, affordable, easy to learn, and capable of functioning under constrained conditions. They do not necessarily need every advanced feature found in multinational chain environments. What they need is reliability in core compliance-relevant functions such as records, payments, permissions, checklists, and evidence retrieval. This suggests that solution quality should be judged by control usefulness and adoption sustainability as much as by feature breadth.

From a policy perspective, the strategic implication is that improving compliance across SME hospitality is not only a private management issue. It has sector-wide consequences for tourist confidence, service quality, digital trust, and formalisation. When smaller hotels are able to meet basic compliance expectations more consistently, the wider destination benefits through stronger standards and lower reputational vulnerability. This creates a justification for policy support mechanisms such as simplified compliance guidance, shared training resources, digital templates, and incentives that lower the cost of secure technology adoption. The literature therefore supports a combined enterprise and ecosystem view of compliance improvement rather than leaving the burden entirely on individual operators (OECD, 2022; UN Tourism, n.d.).

A final strategic implication concerns research and managerial thinking. Compliance in SME hotels should be repositioned from the margins of hospitality technology scholarship to a central theme. Too often, digital transformation research emphasises marketing,

experience, and efficiency while treating compliance as a background issue. The evidence in this review suggests that compliance is actually one of the most practical lenses for understanding the value of technology in resource-constrained hospitality contexts. It links legal expectations, service reliability, internal control, and resilience in a way that is highly relevant for Sri Lankan SME hotels and other emerging market settings alike. This broader framing also supports the paper's conclusion that technology investments create the strongest value when they are designed around evidence readiness, manageable governance, and real operating constraints rather than around abstract notions of digital modernity alone.

Expanded Future Research Directions

Future research should move beyond broad claims that technology improves hospitality operations and instead examine how specific digital capabilities influence distinct compliance outcomes in SME hotel settings. A first priority is measurement development. Compliance is often discussed as a general concept, yet the reviewed studies show it is composed of several domains including data protection, payment control, licensing evidence, hygiene and safety routines, labour-related record keeping, and environmental reporting. Researchers should develop clearer domain-specific indicators so that future work can assess which aspects of compliance improve most through cloud platforms, digital workflows, and baseline security controls.

A second priority is mechanism-based research. Not all technologies strengthen compliance in the same way. A property management system improves centralisation and traceability. Digital payment integration improves reconciliation and financial auditability. Mobile checklists improve routine task visibility. Security controls improve access discipline and incident resilience. Future studies should compare these mechanisms directly, rather than treating technology adoption as a single undifferentiated variable. This would produce more actionable evidence for hotel operators and solution providers who must decide which investments to prioritise under resource constraints.

A third area for research is the role of moderating conditions in the Sri Lankan context. The conceptual framework in this review proposes that finance, skills, infrastructure, policy conditions, and organisational readiness shape the relationship between technology and compliance. Empirical testing of these moderation effects would be valuable. Mixed methods studies could compare hotels with similar size profiles but different levels of digital maturity to explore how governance routines, managerial commitment, and vendor support influence outcomes. Such work would be especially useful for understanding why apparently similar hotels obtain very different results from comparable technologies.

Longitudinal studies would also improve the evidence base. Compliance benefits may not appear immediately after implementation because hotels first experience training demands, workflow changes, and configuration issues. Short-term assessments may therefore underestimate long-run value. Studies that follow adoption over time could identify how compliance routines stabilise, which controls are maintained or abandoned, and what forms of support are needed to sustain benefits. This is particularly relevant in SME settings where staff turnover and shifting business pressure can quickly alter how a system is used.

Comparative work across emerging market tourism settings would add further insight. Sri Lanka shares some characteristics with other destinations where SME hotels dominate and

resource constraints shape digital adoption. Cross-country comparison could reveal which elements of technology-enabled compliance are context-specific and which are more widely transferable. Such work would be useful for theory building around compliance capability, digital maturity, and the organisational conditions required for low-burden but reliable governance in small hospitality firms.

Finally, future research should examine the wider business effects of compliance capability. The literature reviewed here suggests that stronger compliance may contribute indirectly to guest trust, reputation, revenue protection, and resilience. These outcomes are highly relevant for SME hotels, yet they are rarely measured together. Research that models the relationship between technology, compliance capability, and broader business performance would make a strong contribution to hospitality scholarship and offer practical evidence for investment decisions in the Sri Lankan SME sector.

Conclusion and Recommendations

Conclusion

This systematic literature review synthesised 58 eligible sources to examine how cloud computing solutions can support compliance in Sri Lankan SME hotels. The findings indicate that cloud-based systems can strengthen compliance by standardising records, improving traceability, generating auditable evidence, supporting secure data handling, enabling payment reconciliation, and embedding routine compliance checks into hotel operations.

However, technology alone cannot ensure compliance. Its effectiveness depends on suitable system design, staff competence, reliable infrastructure, clearly assigned responsibilities, minimum security controls, and regular internal review. Cloud computing should therefore be viewed as an enabling infrastructure that supports compliance governance rather than as a replacement for managerial responsibility.

The review contributes a structured understanding of technology-enabled compliance within a resource-constrained hospitality context. It provides practical direction for SME hotel operators, policymakers, industry bodies, and technology providers while highlighting the need for empirical research within Sri Lankan hotels (International Organization for Standardization, 2021, 2022; National Institute of Standards and Technology, 2024; Parliament of Sri Lanka, 2022; PCI Security Standards Council, 2024).

Practical Recommendations for Sri Lankan SME Hotel Operators

Based on the synthesis, the following actions are recommended for SME hotel operators seeking practical and affordable improvements in compliance.

1. Prioritise standardisation and evidence readiness - Select core operational systems that create consistent records and time-stamped transactions, and ensure the system can generate exports or reports that support licensing, inspections, and internal monitoring (Ali et al., 2023; Law et al., 2018).
2. Implement minimum security baselines for data protection - Adopt a minimum set of controls that are feasible for SMEs, including role-based access, strong

authentication, logging, backups, patching routines, and an incident response checklist. These practices provide measurable safeguards aligned with recognised security guidance and support compliance readiness for personal data protection expectations (ISO, 2022; National Institute of Standards and Technology, 2024; Parliament of Sri Lanka, 2022).

3. Strengthen financial compliance through integrated payments and reconciliation - Where digital payments are used, ensure payment processes are integrated with operational systems to support reconciliation, exception handling, and traceable audit trails. This improves transparency and reduces fraud and error risks in routine operations (Payment Card Industry Security Standards Council, 2022; PCI Security Standards Council, 2024).
4. Embed operational compliance through workflow tools - Use digital checklists, task assignment, and alert mechanisms for hygiene, safety inspections, preventive maintenance, and staff governance. Workflow-based compliance is particularly useful in SME hotels with limited supervision capacity and frequent staff turnover (Gajjar&Parmar, 2021).
5. Establish a simple governance cadence - Assign basic compliance roles, conduct monthly internal checks, review exceptions, and maintain a small set of documented policies. A light but consistent governance routine improves sustainability of technology-enabled compliance and aligns with compliance management system principles (International Organization for Standardization, 2021).

Recommendations for Policymakers and Industry Bodies

The evidence suggests that SME hotels benefit when compliance requirements are translated into clear, practical guidance and when capability support is provided.

1. Provide simplified compliance guidance and templates for SMEs - Industry bodies can support SMEs by offering standard templates for policies, checklists, and reporting routines that can be implemented with common digital tools.
2. Support SME capability building - Targeted training programmes on digital compliance, basic cybersecurity, data protection awareness, and operational record keeping would reduce adoption barriers and improve compliance outcomes (Fernando & Bandara, 2022).
3. Encourage minimum security baselines aligned to recognised frameworks - Promoting baseline controls aligned to ISO 27001 and NIST CSF guidance can improve consistency and reduce ambiguity for SME operators and technology providers (ISO, 2022; National Institute of Standards and Technology, 2024).

Recommendations for Technology Solution Providers

The review implies that solution design and implementation support strongly influence compliance outcomes in SMEs.

1. Design for traceability and auditability by default- Systems should provide logs, role based access, time-stamped activity records, and simple reporting outputs that directly support compliance evidence needs (Ali et al., 2023; Buhalis & Leung, 2018).
2. Provide SME friendly security features and setup guidance - Security controls should be built in and easy to configure, with clear guidance on minimum safe configurations aligned to recognised best practices (ISO, 2022; National Institute of Standards and Technology, 2024).
3. Offer implementation support and training - Compliance benefits depend on adoption discipline. Providers should include onboarding training, simple policy templates, and periodic check routines as part of deployment support (International Organization for Standardization, 2021).

Limitations of the Review

This review is limited by the scope and availability of published studies specifically addressing Sri Lankan SME hotels. Although the included sources provide valuable cross-contextual insights from hospitality, tourism, technology, and SME settings, the available evidence may not fully capture the operational, regulatory, financial, and technological realities faced by local hotel operators. In addition, differences in research methods, definitions of compliance, geographical settings, and coverage of compliance domains limit the direct comparison and generalisation of findings across the selected sources. The review also relied primarily on English-language published literature, which may have excluded relevant local studies, institutional documents, and practical industry evidence. Finally, the synthesis is based on findings reported in the existing literature and does not directly measure compliance practices or outcomes within Sri Lankan SME hotels. Future empirical research is therefore required to validate the identified themes and assess their practical relevance within the local hospitality context.

Future Research Directions

Future research can strengthen evidence for Sri Lankan SME hotels by empirically testing the pathways identified in this review. Studies may examine how specific technology combinations influence compliance outcomes, such as data protection readiness, audit trail quality, payment control effectiveness, and inspection readiness. Mixed methods research could also explore implementation barriers, governance routines, and the role of training and managerial commitment in sustaining compliance improvements. Comparative studies between SME hotels with different levels of digital adoption would help identify which technology investments yield the highest compliance impact under resource constraints.

References

- Ali, F., Cobanoglu, C., & Ryu, K. (2023). Hospitality technology: A review and future research agenda. *International Journal of Hospitality Management*, 114, Article 103562. <https://doi.org/10.1016/j.ijhm.2023.103562>
- Baumeister, R. F., & Leary, M. R. (1997). Writing narrative literature reviews. *Review of General Psychology*, 1(3), 311–320. <https://doi.org/10.1037/1089-2680.1.3.311>
- Boto García, D. (2023). Hospitality workers' awareness and training about the risks of online crime and the occurrence of cyberattacks. *Journal of Hospitality and Tourism Management*, 55, 240–247. <https://doi.org/10.1016/j.jhtm.2023.04.010>
- Buhalis, D., & Leung, R. (2018). Smart hospitality: Interconnectivity and compliance in the digital age. *Journal of Hospitality and Tourism Technology*, 9(2), 146–164. <https://doi.org/10.1108/JHTT-08-2017-0070>
- DataGuidance. (2024, September 17). *Sri Lanka: DPA publishes circular on application of PDPA in public sector*.
- Data Protection Authority of Sri Lanka. (2024a). *Circular No. 01/2024: Application of the Personal Data Protection Act (PDPA) in the public sector and introduction to the Data Protection Authority*.
- Data Protection Authority of Sri Lanka. (2024b). *Draft Personal Data Protection (Classification of Categories of Personal Data Permitted to Be Processed in a Third Country by a Public Authority as a Specific Controller) Directives*.
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. <https://doi.org/10.2307/2095101>
- Ekanayake, E. M. S., & Abeywardena, G. M. (2022). Role of SMEs in the Sri Lankan hospitality industry: Opportunities and challenges. *Journal of Tourism Economics and Policy*, 6(1), 23–37. <https://doi.org/10.38142/jtep.v2i1>
- European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*.
- Fernando, M., & Bandara, K. (2022). Digital transformation of SMEs in Sri Lanka: Current status, barriers, and strategic recommendations. *Asian Journal of Business and Technology Studies*, 8(2), 45–56.
- Gajjar, H., & Parmar, H. (2021). Regulatory compliance in hospitality: Impacts and management strategies. *Journal of Hospitality and Tourism Research*, 45(4), 812–828. <https://doi.org/10.1177/1096348020977876>
- Gong, Y., & Schroeder, A. (2022). A systematic literature review of data privacy and security research on smart tourism. *Tourism Management Perspectives*, 44, Article 101019. <https://doi.org/10.1016/j.tmp.2022.101019>
- International Organization for Standardization. (2021). *ISO 37301:2021 compliance management systems: Requirements with guidance for use*.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 information security, cybersecurity and privacy protection: Information security management systems: Requirements*.

Jones, P., Hillier, D., & Comfort, D. (2016). Sustainability in the hospitality industry: Some personal reflections on corporate challenges and research agendas. *International Journal of Contemporary Hospitality Management*, 28(1), 36–67. <https://doi.org/10.1108/IJCHM-05-2014-0230>

Karadayi Usta, S. (2024). Cybersecurity risks analysis in the hospitality industry: A stakeholder perspective on sustainable service systems. *Systems*, 12(10), Article 397. <https://doi.org/10.3390/systems12100397>

Law, R., Buhalis, D., & Cobanoglu, C. (2018). Progress on information and communication technologies in hospitality and tourism. *International Journal of Contemporary Hospitality Management*, 26(5), 727–750. <https://doi.org/10.1108/IJCHM-08-2013-0367>

Mariani, M., & Borghi, M. (2021). Innovation in hospitality and tourism industries: A systematic review of the literature. *International Journal of Contemporary Hospitality Management*, 33(3), 927–964. <https://doi.org/10.1108/IJCHM-10-2020-1159>

Marino, M. (2025). Cybersecurity threats and their impact on the hospitality industry. *International Journal of Gaming Hospitality and Tourism*, 5(1).

Mchunu, N. T. (2025). Privacy concerns and information security in e tourism: Business and information management perspective. *Athens Journal of Tourism*, 12(1–2).

Mkhize, A., Mokhothu, K. D., Tshikhotho, M., & Thango, B. A. (2025). Evaluating the impact of cloud computing on SME performance: A systematic review. *Businesses*, 5(2), Article 23. <https://doi.org/10.3390/businesses5020023>

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29).

Nikopoulou, M., Rizou, M., & Tsourgiannis, L. (2023). Determinants of digital transformation in the hospitality industry: TOE factors and digital maturity. *Sustainability*, 15(3), Article 2736. <https://doi.org/10.3390/su15032736>

Nyamwesa, A. (2024). Cloud computing technology adoption: Challenges for SMEs, a case of selected SMEs in Tanzania. *International Journal of Advanced Business Studies*, 3(2), 1–12. <https://doi.org/10.59857/IJABS.3118>

OECD. (2022). *OECD tourism trends and policies 2022*.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo Wilson, E., McDonald, S., McGuinness, L. A., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, Article n71. <https://doi.org/10.1136/bmj.n71>

- Parliament of Sri Lanka. (2022). *Personal Data Protection Act, No. 9 of 2022*.
- Payment Card Industry Security Standards Council. (2022). *Payment Card Industry Data Security Standard (PCI DSS) version 4.0*.
- PCI Security Standards Council. (2024). *PCI security documents library: PCI DSS version 4.0.1*.
- Perera, R., & Weerasinghe, G. (2021). Regulatory compliance and operational risk in Sri Lankan SME hotels: An exploratory study. *South Asian Journal of Tourism and Hospitality Research*, 3(2), 77–91.
- Pipyros, K. (2025). A new cybersecurity risk assessment framework for the hospitality industry. *Worldwide Hospitality and Tourism Themes*.
- Santarsiero, F., Carlucci, D., & Schiuma, G. (2024). Driving digital transformation and business model innovation in tourism through innovation labs: An empirical study. *Journal of Engineering and Technology Management*, 71, Article 101841. <https://doi.org/10.1016/j.jengtecman.2024.101841>
- Sigala, M. (2020). Tourism and COVID 19: Impacts and implications for advancing and resetting industry and research. *Journal of Business Research*, 117, 312–321. <https://doi.org/10.1016/j.jbusres.2020.06.015>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Sri Lanka Tourism Development Authority. (2023a). *Annual report 2023*.
- Sri Lanka Tourism Development Authority. (2023b). *Annual statistical report 2022*. <https://sltda.gov.lk/>
- Sri Lanka Tourism Development Authority. (2023c). *Annual statistical report 2023*.
- Sri Lanka Tourism Development Authority. (2023d). *Year in review 2023*.
- Sri Lanka Tourism Development Authority. (2024). *Tourist hotel process and document requirement*.
- Sri Lanka Tourism Development Authority. (2025). *Tourist hotel registration process and document requirement 2025*.
- Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology*, 8, Article 45. <https://doi.org/10.1186/1471-2288-8-45>
- Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.
- United Nations World Tourism Organization. (2022). *Tourism and sustainability report 2022*. <https://www.unwto.org/>

UN Tourism. (n.d.). *Digital transformation*.

Wang, D., Li, X. R., & Li, Y. (2022). Generation Z's expectations for smart hospitality: A consumer perspective. *Tourism Management*, 88, Article 104406. <https://doi.org/10.1016/j.tourman.2021.104406>

World Economic Forum. (2024). *Travel and tourism development index 2024*.