



BEYOND THE SURFACE: AN INVESTIGATION INTO THE IMPLEMENTATION AND EFFECTIVENESS OF SECURITY MEASURES IN LUXURY HOTELS IN MANILA

Malana, Franklin Cinco¹, Dr. Marlyn Poking-Wacnag²

¹Philippine College of Criminology

²VPAA, NICOSAT Colleges, Inc.

Article DOI: <https://doi.org/10.36713/epra31624>

DOI No: 10.36713/epra31624

ABSTRACT

The hospitality industry continues to face increasingly complex security challenges brought about by evolving physical, operational, and digital threats. This study examined the implementation and effectiveness of security measures in luxury hotels in Manila, recognizing that effective security extends beyond visible safeguards to include well-trained personnel, established policies, appropriate technologies, and coordinated management practices. Guided by the Socio-Technical Systems Theory, the study aimed to assess the extent to which security measures are implemented, evaluate their effectiveness, determine the relationship between implementation and effectiveness, identify challenges encountered by hotel security professionals, and develop a security enhancement framework. A mixed-methods research design was employed, combining quantitative surveys with qualitative interviews involving hotel managers, security managers, supervisors, security personnel and other stakeholders from selected three luxury hotels in Manila. Quantitative data were analyzed using descriptive and inferential statistical methods, while qualitative responses were examined through thematic analysis to provide deeper insights into the findings. The results showed that luxury hotels generally maintain a high level of implementation and effectiveness across key security areas, including physical security, access control, surveillance, emergency preparedness, information security, and personnel management. The findings also revealed a significant positive relationship between the implementation of security measures and their effectiveness. Despite these strengths, participants identified continuing challenges related to cybersecurity, staff development, technology integration, coordination among departments, and the evolving nature of security threats. The study concludes that sustainable hotel security depends on an integrated approach that combines capable personnel, effective leadership, appropriate technology, and continuous improvement to protect guests, employees, and organizational assets.

KEY WORDS: Security Measures, Luxury Hotels, Personnel Security, Physical Security, Document and Information Security

INTRODUCTION

Hotels operate within a distinctive security environment in which openness and accessibility must coexist with the protection of guests, employees, property, and information. Unlike conventional workplaces with relatively controlled access, hotels accommodate continuous movement across public areas such as lobbies, restaurants, function halls, and parking facilities; semi-restricted spaces such as guest floors and recreational amenities; and restricted back-of-house areas including service corridors, loading bays, offices, and staff-only rooms. This operational complexity becomes particularly pronounced in highly urbanized destinations such as Metro Manila, where hotels serve diverse and continuously changing populations of tourists, business travelers, event participants, contractors, delivery personnel, employees, and walk-in customers. The resulting environment creates multiple points of exposure in which physical, organizational, and technological vulnerabilities can intersect.

The hospitality sector has undergone substantial operational transformation since 2020 as establishments responded to health emergencies, changing traveler expectations, and accelerated digitalization. Global tourism recovery initiatives encouraged hotels to adopt low-contact and technology-supported practices, including mobile check-in, QR-based transactions, cashless payments, digital reservations, and technology-assisted guest management. These measures were promoted as mechanisms for restoring traveler confidence and sustaining tourism recovery (UNWTO, 2020; WTTC, 2020). At the same time, however, greater dependence on digital systems has expanded the range of potential vulnerabilities confronting hospitality establishments. Hotels increasingly depend on internet-facing applications, online reservation platforms, electronic payment systems, email, wireless networks, interconnected devices, and third-party service providers. Consequently, security risks are no longer confined to unauthorized physical access or conventional criminal incidents but also encompass cybersecurity, information protection, and privacy-related threats.

This transformation calls for a broader understanding of hotel security. Traditional controls such as security personnel, closed-circuit television (CCTV), access-control systems, alarms, and physical barriers remain essential, but their presence alone does not establish effective security. Hotels also need competent personnel, reliable procedures, accurate incident reporting, emergency



preparedness, cybersecurity controls, and privacy-compliant information practices. Global threat assessments have continued to identify web applications, email systems, and compromised credentials as important avenues for cyberattacks, highlighting risks directly relevant to hospitality organizations that routinely process personal, financial, and transactional information (Verizon, 2024). Accordingly, hotel security is better conceptualized as an integrated system involving personnel, physical infrastructure, organizational processes, and information security, rather than as a collection of visible protective devices.

The international hospitality sector has responded to these emerging risks through safety protocols, operational standards, and risk-management frameworks. During the post-2020 recovery period, international organizations promoted coordinated approaches to safety, health protection, crisis preparedness, and technology use. The UNWTO (2020), for example, emphasized coordinated safety practices and responsible technology use while recognizing the importance of consent and privacy in handling traveler information. Similarly, the WTTC (2020) introduced standardized Safe Travels protocols intended to support consistent health and safety practices across tourism establishments, including hotels. International standards have likewise encouraged organizations to adopt systematic approaches to risk management and organizational resilience (ISO, 2021). Nevertheless, an important concern remains in translating recommended controls into demonstrable security outcomes. Frameworks frequently specify what organizations should implement, but less attention is sometimes given to determining whether those measures actually improve operational performance through indicators such as incident prevention, time-to-detection, response effectiveness, recovery capability, and staff readiness.

This implementation–effectiveness gap is also evident in hospitality research. Studies have documented the widespread use of standard security and safety measures, including surveillance systems, alarms, and front-desk security presence, but the existence of these measures does not necessarily demonstrate their operational effectiveness (Nagaj & Žuromskaitė, 2020). More recent scholarship has similarly identified weaknesses in the measurement of hotel safety and security, including inconsistent indicators, limited contextualization, and the tendency to equate the existence of policies with actual performance (Savita, Rana, & Singh, 2024). Such concerns suggest that security assessment should move beyond determining whether a measure exists toward examining how consistently it is implemented, how personnel operationalize it, and whether it produces meaningful security outcomes.

The Philippine context further demonstrates the need for such an assessment. Since 2020, the Department of Tourism has issued guidelines governing accommodation establishments under changing public health and operational conditions, institutionalizing revised procedures and safety requirements for the hospitality sector (Department of Tourism, 2020, 2021). While these measures strengthened operational compliance, security assessment may become fragmented when health protocols, physical protection, emergency preparedness, cybersecurity, and information privacy are addressed as separate concerns. The issue is particularly important for surveillance and data-management practices. Hotels routinely use CCTV, access records, guest registration systems, reservation databases, and other forms of information collection for safety and operational purposes. The National Privacy Commission (2020, 2024) has emphasized the need for lawful, proportionate, and appropriately governed surveillance and data-processing practices. Thus, hotels face a dual responsibility: protecting guests, employees, and property while ensuring that security practices comply with privacy and data-protection requirements.

The broader Philippine cybercrime environment adds another dimension to this challenge. Public reporting has indicated substantial cybercrime activity in the country, reinforcing the relevance of digital threats to organizations that process personal and financial information (ABS-CBN News, 2025). For hotels, the implications are particularly significant because digital systems are embedded in routine operations, including reservations, payment processing, guest communications, employee systems, and internet access. Consequently, a security incident may affect not only physical safety but also confidentiality, service continuity, financial transactions, and guest trust. Philippine studies conducted during the post-2020 period have provided useful evidence regarding health-protocol implementation and guest perceptions, but much of this literature has focused on compliance and satisfaction rather than comprehensive assessments of security effectiveness across physical, personnel, emergency, cybersecurity, and privacy dimensions (Evangelista & Ylagan, 2022).

These concerns are particularly salient in Metro Manila, where population density, commercial activity, transportation networks, major event venues, and continuous movement of people create a complex operating environment for hotels. Hotels in the National Capital Region accommodate conferences, conventions, banquets, business activities, and other high-volume events, increasing the need for effective access control, crowd management, surveillance, emergency response, and protection against property-related incidents. Local reporting has documented theft incidents associated with hotel environments, demonstrating that conventional property and access risks remain relevant even in established hospitality establishments (GMA Integrated News, 2024). At the same time, reports concerning cybercrime in the region reinforce the relevance of digital threats to organizations operating within Metro Manila (Philippine News Agency, 2023). These conditions indicate that hotel security cannot be adequately understood by examining physical controls alone.

Emergency preparedness presents an additional dimension of hotel security in a densely built urban environment. Fire incidents and other emergencies reported in Metro Manila and surrounding areas underscore the importance of functioning life-safety systems, evacuation procedures, staff competency, and coordination with external emergency responders (Manila Bulletin, 2024). In high-rise and large-capacity hotels, the effectiveness of fire alarms, detectors, sprinklers, emergency exits, and other protective systems depends not only on their availability but also on regular inspection, staff training, emergency drills, communication procedures, and the ability



of personnel to act appropriately under pressure. Hence, the effectiveness of hotel security is ultimately shaped by the interaction between physical resources and human and organizational capabilities.

Despite the proliferation of security measures in hotels, a significant local research gap remains. Hotels may possess comparable visible controls—such as security personnel, CCTV systems, access cards, alarms, and emergency equipment—yet their actual implementation may vary according to management priorities, resource availability, employee turnover, training practices, clientele, operational scale, and organizational culture. More importantly, the presence of a security measure does not necessarily establish that it is consistently applied or capable of producing the intended outcome. There remains limited consolidated, hotel-specific evidence in Metro Manila examining the extent to which security measures are implemented and, more importantly, how effective they are in actual hotel operations. This gap is consequential because security practices that are highly visible may nevertheless provide limited protection when implementation is inconsistent, coordination is weak, personnel are inadequately prepared, or digital and privacy risks are insufficiently addressed.

Against this backdrop, the present study examines hotel security beyond the surface, focusing on the relationship between the implementation of security measures and their perceived effectiveness within selected hotels in Metro Manila. By examining personnel, physical, emergency, and information-security practices within a unified framework, the study seeks to provide evidence on whether established security measures are translated into effective operational practices. The investigation recognizes that hotel security is not simply a matter of installing equipment or complying with prescribed procedures; it involves the capacity of people, processes, technologies, and organizational systems to prevent, detect, respond to, and recover from security threats.

The study also contributes to the broader agenda of building safer, more resilient, and better-governed urban environments. Hotels are an important component of Metro Manila's tourism and economic infrastructure, and their security practices affect not only guests and employees but also businesses, communities, and the wider tourism ecosystem. In this respect, effective and accountable security management is consistent with Sustainable Development Goal 11, which promotes safe and resilient cities, and Sustainable Development Goal 16, which emphasizes effective, accountable, and inclusive institutions. By generating context-specific evidence on the implementation and effectiveness of hotel security measures, the study provides a basis for strengthening security governance, improving operational preparedness, supporting evidence-based management decisions, and promoting a hospitality environment in which safety and security are treated as integral components of sustainable tourism rather than merely as visible features of hotel operations.

Theoretical Framework

The theoretical framework of this dissertation primarily focuses on Socio-Technical Systems (STS) Theory, as this theory primarily becomes the central integrative lens for examining hotel security. STS theory primarily argues that security does not result from a particular technology or action of a person, but rather from the complex interaction between the "social" subsystem and the "technical" subsystem. In a hotel setting in Metro Manila, where there are a significant number of people, the success of a particular security device or mechanism, such as a biometric device or a cybersecurity device, does not lie within the device or the action of a person. Instead, it primarily depends on how a particular device or mechanism is implemented and supported. The study primarily focuses on STS theory as this theory primarily becomes the central integrative lens for examining hotel security, as "implementation quality" primarily becomes the bridge between having a particular security device and achieving a particular security outcome.

In order to add depth without compartmentalizing the theoretical approach, these theories are incorporated structurally as explanatory or contextual sub-components of the STS framework. In this regard, Defense-in-Depth and Security Governance are used to explain the structural aspects of the technical and social subsystem. Defense-in-Depth provides the contextual rationale for the layers of control that overlap in policy, training, and physical aspects of the hotel's security 'web.' Conversely, Security Governance, based on NIST 2024, provides the explanatory theory for the leadership position of the Social subsystem in hotel security risk management. The theories are not used in isolation but rather define the 'Technical' (Defense-in-Depth) and 'Social/Management' (Security Governance) variables that the STS theory attempts to harmonize.

Moreover, the environmental and behavioral factors in the study are mediated through the contextual application of Routine Activity Theory and Crime Prevention Through Environmental Design (CPTED). These are not applied as separate variables in this framework, but rather as specific stressors in the socio-technical ecosystem. Routine Activity Theory is applied to understand the "opportunity" in terms of the layout of the hotel, for example, in terms of areas like hotel lobbies and service corridors, in which social (guardianship) and technical (layout) elements intersect. CPTED is applied as an extension of this logic in terms of understanding the human perception of safety in terms of specific physical design elements. By subordinating these concepts to the STS core concepts, it is ensured that the framework does not become too broad in scope, and instead seeks to understand through specific and specialized concepts how the balance is maintained in terms of socio-technical elements in areas that are at higher risk.

Philosophically, this comprehensive approach is made operational with Pragmatism and Systems Thinking, which provides philosophical justification for mixed-methods evidence. Rather than seeing security as a static checklist, systems thinking considers the hotel as a dynamic system where changing any part of that system, such as implementing a new data privacy policy, affects all other parts of that system. Pragmatism enables the researcher to concentrate on "what works" with survey, interview, and on-site observational



measures that assess implementation fidelity and effectiveness. This approach guarantees that the study remains theoretically grounded in the interface of the social and technical while offering sufficient contextual depth to develop a strong outcomes-based security framework appropriate for Metro Manila hotels.

Statement of the Problem

This study assessed the implementation and effectiveness of security measures in hotels in Metro Manila as a basis for developing a security framework. It examines how security practices are carried out in daily operations and whether these measures produce desired outcomes such as incident reduction, faster response, compliance, and improved safety perceptions. Further, it aims to determine strengths, gaps, and factors influencing performance across governance, personnel, procedures, and physical controls.

Specifically, it sought answers to the following questions:

1. What is the level of implementation of security measures in the hotel in terms of:
 - 1.1 Personnel Security;
 - 1.2 Physical Security; and
 - 1.3 Document and Information Security?
2. Is there a significant difference between the impact of personnel security, physical security, and document and information security on the level of implementation of security measures within the target hotels?
3. What is the level of effectiveness of security measures in the hotel in terms of:
 - 3.1 Personnel Security;
 - 3.2 Physical Security; and
 - 3.3 Document and Information Security
4. Is there a significant difference between the impact of personnel security, physical security, and document and information security on the level of effectiveness of security measures in the target hotels?
5. Is there a significant relationship between the level of implementation of security measures and the level of effectiveness of security measures in the target hotels?
6. How do hotel managers navigate the tension between maintaining an 'open-door' culture of hospitality and implementing increasingly intrusive security technologies to mitigate modern threats like deepfake fraud and unauthorized physical access?
7. Based on the findings of this study, what programs may be proposed to enhance the security measures of the target hotels?

METHODOLOGY

The study employed an explanatory sequential mixed methods design, in which quantitative data were collected and analyzed first, followed by qualitative data to explain and contextualize the quantitative findings (Creswell & Plano Clark, 2018). This design was appropriate because the study sought to measure the implementation and effectiveness of security measures in selected luxury hotels while also exploring how hotel managers experienced and managed the integration of security requirements with guest-centered hospitality.

The quantitative phase addressed Research Questions 1 to 5 through structured survey questionnaires administered to hotel personnel and guests/visitors. The quantitative findings established the levels of implementation and effectiveness of security measures and provided the basis for the subsequent qualitative inquiry. The qualitative phase, which addressed Research Question 6, involved semi-structured interviews with hotel managers to explain the factors underlying the quantitative results. Particular attention was given to how managers balanced guest satisfaction and an open hospitality environment with increasingly stringent security requirements, including responses to emerging risks such as deepfake fraud and unauthorized physical access. The interview data were analyzed thematically to identify operational challenges, management strategies, and practices that explained and enriched the quantitative findings.

The integration of both phases addressed Research Question 7, which focused on the development of a security enhancement program. Quantitative findings identified strengths and areas requiring improvement, while qualitative findings contributed contextual and practical insights into security management, emergency preparedness, operational coordination, privacy protection, and guest-centered security. Thus, the mixed methods approach provided a more comprehensive understanding of hotel security by combining measurable evidence with the experiences and perspectives of those directly involved in its implementation.

The study involved **192 quantitative respondents** from three selected luxury hotels in Metro Manila: **Solaire Resort North (Quezon City), Solaire Parañaque, and Okada Manila**. The respondents consisted of departmental managers, security personnel, and hotel guests/visitors. Departmental managers and security personnel were selected through **total enumeration**, ensuring the inclusion of all qualified members of these groups. Guests and visitors were selected through **convenience sampling**, considering their transient nature and availability during the data-collection period.

For the qualitative phase, **15 hotel managers**, with five representatives from each participating hotel, served as key informants. Although 20 managers were initially identified as eligible, 15 participated in the in-depth interviews. They were selected based on their



managerial roles and direct involvement in security implementation, supervision, incident management, and the delivery of guest services. Their experiences provided essential contextual evidence for explaining the quantitative findings and informing the proposed security enhancement program.

Table 1. Population of the Study

Hotel	Solaire Quezon City	Solaire Parañaque	Okada Manila	Total
Departmental Managers	15	28	20	63
Security Personnel	15	25	20	60
Guests/Visitors	16	33	20	69
Total	46	86	60	192

The study utilized a **structured survey questionnaire** to measure the implementation and effectiveness of hotel security measures in terms of **personnel security, physical security, and document and information security**. The instrument comprised two major constructs measured through a four-point Likert scale and was developed from relevant security-management literature, international standards, and Philippine laws and regulations, including the Data Privacy Act of 2012, Cybercrime Prevention Act of 2012, Revised Fire Code of the Philippines, Department of Tourism requirements, National Privacy Commission guidelines, and ISO/IEC 27001 principles. A **semi-structured interview guide** was likewise used during the qualitative phase to obtain in-depth perspectives from hotel managers regarding their experiences, challenges, and strategies in balancing hospitality and evolving security requirements. Interview data were analyzed thematically following Braun and Clarke's (2006) approach to provide contextual explanations for the quantitative findings.

Both instruments underwent **expert validation by three specialists** in security management, hospitality management, and research methodology to assess clarity, relevance, completeness, organization, and alignment with the study's objectives and applicable standards. The revised questionnaire was pilot-tested among **30 managers, security personnel, and guests/visitors** from SEDA Hotel Vertis North, who were not included in the actual study. Reliability analysis using **Cronbach's alpha yielded a coefficient of 0.89**, indicating good internal consistency (George & Mallery, 2019). The validation and reliability results established that the survey questionnaire was appropriate for measuring the study variables, while the validated interview guide supported the collection of credible and contextually rich qualitative data. Together, the instruments strengthened the consistency, validity, and trustworthiness of the study's findings.

The quantitative data were analyzed using statistical techniques appropriate for the **four-point ordinal Likert-scale data** and the explanatory sequential mixed-methods design. For **Research Questions 1 and 3**, the **median** was used to determine the levels of implementation and effectiveness of personnel security, physical security, and document and information security. Median scores were interpreted using four descriptive categories: 3.26–4.00 as *Fully Implemented/Very Effective*, 2.51–3.25 as *Implemented/Effective*, 1.76–2.50 as *Slightly Implemented/Slightly Effective*, and 1.00–1.75 as *Not Implemented/Not Effective* (Boone & Boone, 2012; Field, 2018). For **Research Questions 2 and 4**, the **Kruskal-Wallis H test** was used to determine significant differences in implementation and effectiveness across the three participating luxury hotels, with significance tested at the 0.05 level. For **Research Question 5**, **Spearman's rank-order correlation (ρ)** was employed to determine the strength and direction of the relationship between security-measure implementation and effectiveness, with the corresponding *p*-value used to determine statistical significance at the 0.05 level (Schober et al., 2018).

For **Research Question 6**, qualitative interview data were analyzed using **Braun and Clarke's (2006) six-phase thematic analysis**. The process involved familiarization with the interview data, generation of initial codes, searching for themes, reviewing themes, defining and naming themes, and producing the final report. The analysis focused on hotel managers' experiences in balancing guest-centered hospitality with increasingly stringent security measures and emerging threats, including deepfake fraud and unauthorized physical access. Representative participant quotations were used to support the identified themes. Finally, the qualitative findings were integrated with the quantitative results to explain and contextualize the statistical patterns, identify underlying operational and managerial factors, and provide a more comprehensive understanding of hotel security management. This integration strengthened the explanatory value and overall credibility of the mixed-methods findings.

RESULTS AND DISCUSSIONS

This section presents presents, analyzes, and interprets the data gathered from the respondents.

Level of implementation of Security Measures in the Selected Luxury Hotels

Personnel Security. The area on **personnel security was Fully Implemented across the selected luxury hotels (overall Median = 4.00)**, with the same median obtained across all ten indicators and among Solaire Quezon City, Solaire Parañaque, and Okada Manila. The findings demonstrate consistent implementation of employee background screening, security awareness and emergency-response training, staff identification and access-control procedures, roving security patrols, threat-intelligence briefings, behavioral



observation, incident reporting, and monitoring of third-party contractors. This uniformity suggests that personnel security has been institutionalized through standardized procedures and management practices aimed at minimizing insider threats, unauthorized access, human-factor vulnerabilities, and operational disruptions. The findings are consistent with ISO/IEC 27001:2022 and Kassem (2024), which emphasize systematic risk management, employee accountability, and personnel screening, as well as IBM Security (2024) and Verizon (2024), which underscore employee awareness and preparedness as important safeguards against security incidents. The results also support the NDRRM Plan 2020–2030, which emphasizes continuous training, defined responsibilities, and emergency preparedness. The use of roving security personnel further reinforces the importance of combining human vigilance with technology, consistent with Rocamora (2021) and Savita and Singh (2024), while regular threat briefings and behavioral observation reflect the need for context-sensitive threat intelligence and continuous risk assessment (Muir Analytics, 2022; ENISA, 2024; CrowdStrike, 2025). Formal reporting mechanisms likewise align with the governance and coordinated incident-management principles of NIST CSF 2.0 and NDRRMC Operations Center (2021).

The qualitative findings corroborated the uniformly high quantitative results by demonstrating how personnel security measures are operationalized in everyday hotel activities. Managers described consistent application of security procedures while maintaining professionalism, guest comfort, and privacy. For example, HM 1 explained that a VIP guest who initially resisted security inspection was persuaded to cooperate through calm communication and an explanation that the policy applied equally to all guests. Similarly, HM 2 and HM 6 described identity verification and visitor-registration procedures, while HM 7 emphasized authorization checks for elevator and restricted-area access. HM 13 summarized the practice as, “*Identity muna, bago binigyan ng room access*,” reflecting the priority given to verification before granting access. Managers also highlighted discretion in handling VIPs, celebrities, media representatives, and sensitive incidents. HM 5 noted that celebrity arrivals were managed discreetly, while HM 10 described quietly redirecting media representatives during a VIP event to protect guest privacy. HM 15 further emphasized that security monitoring and intervention were communicated as measures intended to enhance safety rather than intrude on guests. Collectively, these accounts explain the quantitative finding by showing that personnel security in the participating hotels extends beyond the presence of security personnel and formal procedures; it involves competent personnel, consistent enforcement, effective communication, discretion, privacy protection, and guest-centered security practices. Thus, the evidence indicates that the high level of personnel security implementation is embedded in routine operational practices and supported by a management approach that seeks to reconcile rigorous security requirements with the expectations of luxury hospitality.

Physical Security. Physical security measures were **Fully Implemented (overall Median = 4.00)** across the selected luxury hotels, with all ten indicators likewise receiving a median of 4.00. The findings indicate consistent implementation of CCTV surveillance, electronic RFID locks, vehicle barriers, baggage screening, adequate lighting, property zoning, intrusion alarms, fire and life-safety equipment, strategically positioned security stations, and strict master-key controls. This consistency suggests that the participating hotels have institutionalized layered physical security practices designed to prevent unauthorized access, deter criminal activity, protect assets, and support emergency response while maintaining guest convenience. The findings are consistent with National Privacy Commission (2024), DivinaLaw (2024), and Gorriceta Law (2025), which emphasize that effective CCTV security requires appropriate governance, controlled access, documentation, and accountability. Property zoning, adequate lighting, and layered access controls further reflect defense-in-depth principles, while visible security stations support guest confidence and operational continuity (American Hotel & Lodging Association, 2020; Department of Tourism, 2023). The literature also demonstrates the continuing importance of active access control and human intervention, as inadequate identity verification and reliance on surveillance alone may leave hotel guests vulnerable to security incidents (Rawlinson, 2026; Reuters, 2023; Rocamora, 2021). Thus, the findings suggest that physical security in the participating hotels functions as an integrated system in which technology, infrastructure, personnel, and operational procedures work together to protect guests, employees, and hotel assets.

The qualitative findings reinforced these results by demonstrating how physical security measures are applied in actual hotel operations while preserving the guest experience. Managers described the use of CCTV as a safety and investigative tool while emphasizing privacy, with HM 15 explaining that its purpose was to improve safety rather than invade guests' privacy. Strict access-control procedures were likewise evident in identity verification before replacement room keys were issued and before access to restricted areas was granted. HM 13 summarized the practice as, “*Identity muna, bago binigyan ng room access*,” while HM 7 described authorization checks for elevator access. Managers also provided accounts of coordinated responses to fire alarms, suspicious packages, bomb threats, and gas leaks, including orderly evacuation, relocation, continuous communication, and reassurance of guests. Visible security presence was similarly maintained during high-volume activities, with HM 6 noting that security coordination and identity verification continued even during large group check-ins. Collectively, these narratives show that physical security extends beyond the installation of protective technologies; its effectiveness depends on consistent access control, active monitoring, emergency readiness, coordinated personnel response, and discreet enforcement. The integration of these practices enables luxury hotels to maintain a secure environment while minimizing disruption to the guest experience.

Document and Information Security. Document and information security measures were **Fully Implemented (overall Median = 4.00)** across the selected luxury hotels, with all ten indicators likewise obtaining a median of 4.00. The findings indicate that



the hotels have institutionalized comprehensive controls for protecting guest, employee, and organizational information. These include strong password policies and multi-factor authentication, encrypted networks, regular data backups, secure disposal of confidential documents, role-based access to the Property Management System (PMS), firewall and anti-malware protection, proper classification and storage of sensitive records, Non-Disclosure Agreements (NDAs), secure payment processing, and periodic auditing of digital access logs. This consistent implementation reflects the integration of information security into routine hotel operations and supports the protection of personal and financial information, operational continuity, and guest confidence. The findings are consistent with ISO/IEC 27001:2022, NIST SP 800-53 Rev. 5, PCI DSS v4.0, the National Privacy Commission, and the DICT National Cybersecurity Plan 2023–2028, which emphasize access control, authentication, data protection, monitoring, accountability, and organizational resilience. They also align with Microsoft Digital Defense Report (2024), Verizon (2024; 2025), IBM Security (2024), ENISA (2024), and CrowdStrike (2025), which underscore the continuing risks associated with compromised credentials, human error, unauthorized access, and evolving cyber threats.

The qualitative findings reinforced the quantitative results by demonstrating how information security principles were applied through everyday hotel practices. HM2 reported that lost room keys were replaced only after guest identities were verified, while HM13 emphasized, *“Identity muna, bago binigyan ng room access,”* with passports and other valuable documents returned only after confirming the rightful owner. These practices reflect controlled access and verification consistent with information-security principles. HM15 likewise described explaining the purpose of CCTV monitoring as improving safety and supporting investigations rather than invading guest privacy, illustrating responsible handling of sensitive information. The managers' emphasis on discretion when handling VIP and celebrity guests and confidentiality in sensitive incidents further reflected an organizational culture of privacy and trust. Overall, the findings suggest that document and information security extends beyond technical safeguards to encompass employee accountability, controlled access, privacy-conscious practices, and professional discretion. Sustaining these measures through continuous cybersecurity training, system monitoring, vulnerability assessment, software updating, and periodic security testing will be important as digital threats to hospitality operations continue to evolve.

Significant Difference in the Level of Implementation of Security Measures in the Selected Luxury Hotels in terms of Identified Variables According to Hotels

The Kruskal–Wallis H test showed no statistically significant differences in the implementation of personnel, physical, and document and information security measures among Solaire Quezon City, Solaire Parañaque, and Okada Manila. Personnel security yielded $H = 2.869$, $p = .238$; physical security yielded $H = 0.416$, $p = .812$; and document and information security yielded $H = 2.039$, $p = .361$. Since all p -values exceeded the .05 significance level, the null hypothesis was not rejected for all three dimensions. Thus, respondents across the three hotels reported statistically comparable levels of security implementation. This result is consistent with the descriptive findings, in which all three dimensions obtained an overall median of 4.00 (Fully Implemented), indicating that the selected hotels followed broadly similar security practices.

Table 2. Significant Difference in the Level of Implementation of Security Measures in the Selected Luxury Hotels in terms of Identified Variables According to Hotels

Dimension	Kruskal-Wallis H	df	p-value	Decision	Interpretation
Personnel Security	2.869	2	0.238	Fail to Reject H_0	There is no significant difference in the level of personnel security implementation among the three hotels.
Physical Security	0.416	2	0.812	Fail to Reject H_0	There is no significant difference in the level of physical security implementation among the three hotels.
Document and Information Security	2.039	2	0.361	Fail to Reject H_0	There is no significant difference in the level of document and information security implementation among the three hotels.

The absence of significant differences is consistent with the standardization promoted by NIST CSF 2.0, ISO/IEC 27001:2022, CIS Controls v8, and PCI DSS v4.0, which emphasize systematic governance, access control, monitoring, protection, and continuous improvement. It also accords with Savita and Singh (2024), who emphasized the integration of personnel, technology, and operational procedures in hotel security, and Muir Analytics (2022), which noted that luxury hotels may adapt controls to local risks while retaining common foundational security practices. In the Philippine context, the Department of Tourism's operating standards and the Safety Seal Certification Program likewise establish common safety and security expectations for accommodation establishments. The comparable



implementation observed across the three hotels may therefore reflect shared industry standards, regulatory requirements, risk profiles, and organizational expectations for guest and asset protection.

Overall, the findings indicate that the selected luxury hotels maintained comparable and standardized security implementation across personnel, physical, and document and information security. Given the uniformly high level of implementation, future efforts may focus less on increasing the presence of basic controls and more on strengthening their effectiveness, resilience, and adaptability through continuous security audits, employee development, technological updating, and preparedness for emerging risks such as cyberattacks, insider threats, AI-enabled fraud, and evolving physical security challenges.

Level of effectiveness of security measures in the Selected Luxury Hotels

Personnel Security. Personnel security measures were perceived as **Very Effective (overall Median = 4.00)** across the selected luxury hotels, with all ten indicators likewise obtaining a median of 4.00. The findings indicate that personnel security practices were not only fully implemented but were also perceived to effectively achieve their intended objectives. These included employee background screening, security awareness and emergency response training, staff identification and access control, roving security, threat intelligence briefings, behavioral observation, incident reporting, and supervision of contractors and vendors. The consistently high ratings suggest that security responsibilities were embedded in routine operations through employee competence, accountability, preparedness, and adherence to established procedures. These findings are consistent with Nagaj and Žuromskaite (2020), Torralba and Ylagan (2021), and Felicen et al. (2020), who emphasized the importance of competent personnel, continuous training, and preparedness in hotel security. They also support Karadayi-Usta (2024) and Verizon (2024), which highlighted the importance of access control, clearly defined responsibilities, and human-factor security in reducing organizational vulnerabilities.

The qualitative findings further explained how personnel security was translated into effective operational practice. HM3 noted that experience in medical emergencies and evacuations strengthened *“clear communication and quick coordination,”* while HM8 described improved teamwork and timely communication that kept guests informed and cooperative during emergencies. HM15 likewise reported strengthened evacuation procedures, communication, and coordinated teamwork. Managers also emphasized the importance of verification and access control. HM1 stated that experience led to greater focus on *“prioritizing verification while ensuring that service remained fast and efficient,”* while HM10 described improving access enforcement without making guests uncomfortable. These accounts demonstrate that effectiveness depended not only on procedural compliance but also on communication, professionalism, teamwork, courtesy, and situational awareness. As HM1 expressed, *“hospitality and security should always work together rather than compete with each other.”* Overall, the findings suggest that personnel security is most effective when competent and well-prepared employees integrate security responsibilities with guest-centered service. Sustaining this effectiveness requires continuous training, competency assessment, emergency simulations, threat-awareness activities, and periodic updating of personnel security procedures to address emerging risks such as insider threats, social engineering, and AI-enabled fraud.

Physical Security. Physical security measures were perceived as Very Effective (overall Median = 4.00) across the selected luxury hotels, with all ten indicators likewise obtaining a median of 4.00. The findings indicate that surveillance systems, RFID-based electronic locks, vehicle barriers, baggage screening, adequate lighting, property zoning, intrusion alarms, fire and life-safety equipment, strategically positioned security desks, and master-key controls were perceived to function effectively in protecting guests, employees, facilities, and organizational assets. The consistently high ratings suggest that physical security has been integrated into routine hotel operations through the coordinated use of infrastructure, technology, procedures, and personnel oversight. These findings are consistent with Nagaj and Žuromskaite (2020), Torralba and Ylagan (2021), and Abad et al. (2025), which emphasize that effective hotel security depends on the integration of physical infrastructure, personnel capability, and operational procedures. They also support Muir Analytics (2022), Unsaflok (2024), and ASIS International (2024), which underscore the importance of continuous maintenance, security assessment, and appropriate management of electronic access-control systems. Visible and consistently maintained security measures may likewise contribute to guest confidence and perceptions of safety (Bartolome, 2023; Tourism Management, 2020).

The qualitative findings further explained how physical security measures were translated into effective practice. Managers emphasized that access-control technologies were reinforced by consistent identity verification and professional enforcement. HM1 reported *“prioritizing verification while ensuring that service remained fast and efficient,”* while HM11 noted that essential identity-verification procedures were not skipped even when faster service was required. HM10 similarly described improving access enforcement without making guests uncomfortable. The effectiveness of property zoning was reflected in HM4's account of ensuring that only authorized individuals entered secure areas while minimizing disruption to hotel operations. HM6 also described coordinated check-in and event registration procedures that balanced efficient service with required security verification. These accounts demonstrate that the effectiveness of physical security depends not only on the presence of technological and structural controls but also on their consistent application by personnel. As HM5 summarized, *“When security is implemented professionally and with compassion, it builds guest trust and strengthens both safety and the hotel's reputation.”* Overall, the findings suggest that physical security is most effective when surveillance, access control, environmental safeguards, emergency infrastructure, and personnel practices operate as an integrated system supported by clear communication, coordination, and guest-centered service. Sustaining this effectiveness requires preventive



maintenance, regular system testing and security assessments, and appropriate modernization to address evolving physical and technology-enabled threats.

Document and Information Security. Document and information security measures were perceived as **Very Effective (overall Median = 4.00)** across the selected luxury hotels, with all ten indicators likewise obtaining a median of 4.00. The findings indicate that controls for authentication, encryption, data backup, secure document disposal, role-based access to the Property Management System (PMS), firewall and anti-malware protection, confidential document handling, Non-Disclosure Agreements (NDAs), secure payment processing, and digital access-log auditing were perceived to function effectively in protecting guest, employee, and organizational information. The consistently high ratings suggest that information security has been integrated into routine hotel operations through technical safeguards, governance procedures, employee accountability, and privacy-conscious practices. These findings are consistent with Microsoft (2024), Verizon (2024), IBM Security (2024), Karadayi-Usta (2024), ENISA (2024), and the National Privacy Commission (2023; 2024), which emphasize strong authentication, access control, employee awareness, secure information handling, monitoring, and organizational accountability. They also align with ISO/IEC 27001:2022, NIST SP 800-53 Rev. 5, and PCI DSS v4.0, which promote systematic protection of information assets, secure transactions, continuous monitoring, and organizational resilience. Philippine reports documenting increasing phishing, booking fraud, identity theft, and online scams further underscore the importance of maintaining these controls.

The qualitative findings provided additional evidence for the human and procedural dimensions of information security. HM1 emphasized *“prioritizing verification while ensuring that service remained fast and efficient,”* while HM11 reported that essential identity-verification procedures were not skipped, even when faster guest processing was required. These accounts reinforce the principle of restricting access to authorized individuals. Managers also emphasized confidentiality and privacy in handling sensitive guest information. HM4 described more discreet security arrangements for VIP guests, while HM9 and HM14 stressed privacy when handling guest belongings and coordinating with media during VIP events. These narratives demonstrate that information protection extends beyond technological safeguards to include confidentiality, controlled access, professional discretion, and responsible handling of guest information. However, the interviews did not directly address specific technical controls such as password policies, multi-factor authentication, encryption, firewall and anti-malware systems, secure payment gateways, or digital access-log auditing. Thus, the qualitative phase primarily corroborated the human and procedural aspects of the quantitative findings rather than independently validating the technical controls. Overall, the convergence of the two phases indicates that effective document and information security depends on the integration of technology, governance, personnel practices, and privacy-conscious service. Sustaining this effectiveness requires continuous cybersecurity awareness, vulnerability assessment, system monitoring, policy review, and preparedness for emerging threats such as ransomware, phishing, insider risks, and AI-enabled fraud.

Significant Difference in the Level of Effectiveness of Security Measures in the Selected Luxury Hotels in terms of Identified Variables According to Hotels

Table 3 presents the results of the Kruskal–Wallis H test conducted to determine whether significant differences exist in the perceived effectiveness of security measures among Solaire Quezon City, Solaire Parañaque, and Okada Manila. The findings reveal that no statistically significant differences exist among the three hotels across all security dimensions.

The Kruskal–Wallis H test revealed **no statistically significant differences** in the perceived effectiveness of personnel, physical, and document and information security measures among the three selected luxury hotels. Personnel security yielded $H = 1.092$, $p = .579$; physical security yielded $H = 1.706$, $p = .426$; and document and information security yielded $H = 2.159$, $p = .340$. Since all p -values exceeded the .05 significance level, the null hypothesis was not rejected for any dimension. Thus, respondents across the three hotels had statistically comparable assessments of security effectiveness. This result complements the descriptive findings, where all three dimensions obtained an overall median of 4.00 (Very Effective), suggesting that the security measures were perceived as similarly effective regardless of hotel location.

**Table 3. Significant Difference in the Level of Effectiveness of Security Measures in the Selected Luxury Hotels in terms of Identified Variables According to Hotels**

Dimension	Kruskal-Wallis H	df	p-value	Decision	Interpretation
Personnel Security	1.092	2	0.579	Fail to Reject H_0	There is no significant difference in the perceived effectiveness of personnel security among the three hotels
Physical Security	1.706	2	0.426	Fail to Reject H_0	There is no significant difference in the perceived effectiveness of physical security among the three hotels
Document and Information Security	2.159	2	0.340	Fail to Reject H_0	There is no significant difference in the perceived effectiveness of document and information security among the three hotels.

The absence of significant differences is consistent with the standardization promoted by internationally recognized security and hospitality practices. NIST CSF 2.0, ISO/IEC 27001:2022, and related cybersecurity frameworks emphasize systematic governance, access control, continuous monitoring, and organizational accountability, while studies by Nagaj and Žuromskaite (2020), Torralba and Ylagan (2021), and Karadayi-Usta (2024) highlight the importance of integrating personnel, infrastructure, technology, and operational procedures. Similarly, Abad et al. (2025), Sisneros et al. (2025), and Algario et al. (2024) emphasized that consistent training, infrastructure maintenance, emergency preparedness, and management oversight contribute to effective hotel safety and security. The comparable effectiveness observed may therefore reflect shared industry expectations, regulatory requirements, standardized procedures, and common security technologies across luxury hospitality establishments.

The qualitative findings further explained the statistical similarity. Managers across the three hotels consistently emphasized professionalism, communication, empathy, identity verification, access control, emergency coordination, and guest privacy. HM1 noted that security procedures should be explained “*with respect and courtesy*,” emphasizing that “*hospitality and security should always work together rather than compete with each other*.” HM2 similarly observed that remaining “*kalmado at magalang*” encouraged guest cooperation, while HM3 and HM8 described clear communication and coordinated teamwork as essential during emergencies. For information security, HM4, HM9, and HM14 emphasized discreet handling of VIP arrangements, verification of ownership, and protection of guest confidentiality. Although the interviews provided limited direct evidence concerning technical controls such as encryption, firewalls, and password management, they consistently demonstrated common human and procedural approaches to security across the participating hotels.

Overall, the quantitative and qualitative findings converge in indicating comparable effectiveness across personnel, physical, and document and information security. Rather than reflecting substantial differences among properties, the findings suggest that security has been institutionalized through common professional standards, coordinated procedures, trained personnel, physical safeguards, information controls, and management oversight. Given the uniformly Very Effective assessments, continued attention may focus on sustaining and adapting these systems through regular audits, professional development, infrastructure maintenance, cybersecurity monitoring, and preparedness for emerging risks such as insider threats, cybercrime, AI-enabled fraud, and evolving physical security challenges.

Significant Relationship Between the Level of Implementation of Security Measures and the Level of Effectiveness of Security Measures in the Target Hotels

Table 4 presents the results of the Spearman's rank-order correlation (Spearman's ρ) analysis conducted to determine whether a significant relationship exists between the level of implementation and the level of effectiveness of security measures in the selected luxury hotels. Spearman's rho was employed because the study used ordinal data obtained from a four-point Likert scale, making it an appropriate nonparametric statistical test for assessing the strength and direction of association between two ranked variables.

The findings revealed significant positive relationships between implementation and effectiveness across all security dimensions. Personnel Security showed a strong relationship ($\rho = 0.713$, $p < .001$), Physical Security a moderate-to-strong relationship ($\rho = 0.684$, $p < .001$), and Document and Information Security a moderate relationship ($\rho = 0.570$, $p < .001$). Overall, implementation and effectiveness demonstrated a very strong relationship ($\rho = 0.821$, $p < .001$). Since all p-values were below .05, the null hypothesis was rejected. The results indicate that consistently implemented security policies, procedures, personnel practices, and technologies are associated with greater perceived security effectiveness.



The qualitative findings explained these relationships through managers' experiences of professional communication, consistent identity verification, discreet enforcement, coordinated emergency response, and privacy protection. For Personnel Security, HM 1 noted that calmly explaining inspection policies encouraged guest cooperation, while HM 15 emphasized professionalism, empathy, and *"maayos na communication."* HM 13 similarly stressed, *"Identity muna, bago binigyan ng room access."* For Physical Security, managers described coordinated access control and emergency response, with HM 3 emphasizing that *"clear communication and quick coordination are essential."* For Document and Information Security, managers highlighted discreet handling of VIP information, confidentiality, and privacy-conscious CCTV practices. These accounts indicate that security measures become more effective when procedures are applied consistently, professionally, and with sensitivity to guest needs.

The findings support the Socio-Technical Systems Theory, demonstrating that security effectiveness depends on the interaction of people, organizational processes, and technology. They also align with Security Governance, Defense-in-Depth, Routine Activity Theory, and Crime Prevention Through Environmental Design, particularly in emphasizing management oversight, capable personnel, layered safeguards, effective guardianship, surveillance, and controlled access. The results are likewise consistent with the objectives of Republic Act No. 9514, Republic Act No. 10173, Republic Act No. 10175, Executive Order No. 58, and relevant Department of Tourism and National Privacy Commission requirements concerning safety, privacy, cybersecurity, and security management.

Overall, the quantitative and qualitative findings demonstrate convergence: stronger implementation was associated with greater effectiveness, while managerial experiences explained the operational practices underlying this relationship. The results underscore the importance of consistent policy enforcement, personnel competency, regular training, maintenance of physical and technological safeguards, privacy protection, and continuous monitoring. For luxury hotels, an integrated security management approach that combines leadership, people, technology, procedures, and regulatory compliance is therefore essential to sustaining both security effectiveness and quality guest service.

Hotel Managers Navigating the Tension Between Maintaining an 'Open-door' Culture of Hospitality and Implementing Increasingly Intrusive Security Technologies to Mitigate Modern Threats

Using Braun and Clarke (2006), this section presents the themes generated based on the actual statements of the fifteen hotel managers of the luxury hotels (Solaire Quezon City, Solaire Parañaque, and Okada Manila) from the three probing questions which include "Can you describe a specific experience where you had to balance guest hospitality with security measures?," "What challenges did you experience while trying to make guests feel welcome and keep the hotel secure?," and "How did that experience influence the way you manage hospitality and security in your hotel?."

Experiences in Balancing Guest Hospitality with Security Measures. The hotel managers' narratives revealed five interconnected themes describing how security measures were balanced with the expectations of luxury hospitality: (1) Respectful Communication and Professionalism Foster Guest Acceptance of Security Measures; (2) Consistent Identity Verification and Access Control Ensure Guest Safety While Maintaining Hospitality; (3) Discreet Security Enforcement Maintains Safety Without Disrupting the Guest Experience; (4) Calm, Coordinated Emergency Response Enhances Guest Safety and Confidence; and (5) Protecting Guest Privacy While Implementing Security Strengthens Guest Confidence. Collectively, the themes indicate that effective hotel security depends not only on physical and technological safeguards but also on communication, professionalism, consistency, discretion, and respect for guest privacy.

Theme 1: Respectful Communication and Professionalism Foster Guest Acceptance of Security Measures. Managers emphasized that guests were more willing to cooperate when security procedures were explained calmly, fairly, and courteously. HM 1 recalled how calmly explaining an inspection policy to a VIP guest resulted in cooperation, while HM 15 stressed the importance of professionalism, empathy, and *"maayos na communication"* in balancing hospitality and security. Similarly, HM 5 described discreetly managing celebrity check-in procedures, and HM 10 explained that media personnel were redirected respectfully during VIP events to protect guest privacy. These experiences demonstrate that clear and respectful communication can transform potentially intrusive security procedures into trust-building interactions. The findings are consistent with Hernandez-Calderon (2021), Tourism Management (2020), and Karadayi-Usta (2024), which emphasize communication, stakeholder coordination, and consistent security practices as important factors in guest acceptance and confidence.

Theme 2: Consistent Identity Verification and Access Control Ensure Guest Safety While Maintaining Hospitality. Managers described the consistent verification of room keys, visitor registrations, event credentials, restricted-area access, and reservations, even during busy operations. HM 2 noted that politely explaining verification requirements helped guests understand the need for additional procedures, while HM 13 emphasized, *"Identity muna, bago binigyan ng room access."* HM 6 similarly reported that guest identities were verified before room keys were issued during large-group check-ins. These experiences indicate that access controls are more acceptable when applied uniformly, professionally, and without unnecessary disruption. The findings are consistent with Karadayi-Usta (2024), Microsoft (2024), Verizon (2024), IBM Security (2024), and Torralba and Ylagan (2021), which emphasize identity management, access control, employee competence, and consistent implementation as essential elements of organizational security.



Overall, the first two themes demonstrate that security and hospitality are not necessarily competing priorities. Rather, security measures become more effective and acceptable when implemented through professional communication, consistent verification, and guest-centered service. The managers' experiences further suggest that frontline personnel play a critical role in translating security policies into practices that protect guests while preserving the welcoming character of luxury hospitality.

Theme 3: Discreet Security Enforcement Maintains Safety Without Disrupting the Guest Experience. Managers described handling security concerns through unobtrusive interventions that protected guests without creating unnecessary alarm. HM 3 reported politely redirecting intoxicated guests from restricted areas, controlling unauthorized room-access requests, regulating delivery personnel, and discreetly monitoring suspicious individuals. HM 8 similarly described securing a theft scene while preventing guest panic, while HM 14 emphasized professionally managing vehicle checkpoints, unauthorized photography, and blocked emergency exits. These experiences indicate that effective security need not be intimidating or highly visible; rather, professional judgment, situational awareness, and courteous intervention can protect guests while preserving the atmosphere of luxury hospitality. The findings are consistent with Nagaj and Žuromskaite (2020), Tourism Management (2020), Hernandez-Calderon (2021), and Torralba and Ylagan (2021), who emphasized that security is most effective when integrated into hotel operations without unnecessarily compromising guest comfort. They also support Abad et al. (2025), Sisneros et al. (2025), and Bartolome (2023), which highlight the importance of personnel competence, preparedness, and professional handling of security incidents. Overall, the theme demonstrates that discreet enforcement strengthens both security and guest confidence by minimizing disruption while maintaining vigilance.

Theme 4: Calm, Coordinated Emergency Response Enhances Guest Safety and Confidence. Managers consistently emphasized calm communication, teamwork, and prompt action during emergencies. HM 4 described coordinated responses to suspicious packages, fire alarms, missing children, and power outages, while HM 9 recounted managing medical emergencies and bomb threats through calm leadership and continuous communication. HM 12 likewise highlighted immediate interdepartmental coordination during missing-child and gas-leak incidents. These experiences show that emergency effectiveness depends not only on established procedures but also on personnel readiness, coordination, and the ability to reassure guests during stressful situations.

The findings support Felicen et al. (2020), Algario et al. (2024), Pipyros and Liasidou (2025), and GJETA (2021), which emphasize continuous training, emergency drills, clearly defined responsibilities, organizational readiness, and coordinated response. They are also consistent with the incident-response principles discussed by Mandiant (2024; 2025) and CrowdStrike (2025), particularly rapid detection, communication, and coordinated action. Thus, regular preparedness activities and crisis-communication training are essential for protecting both guest safety and confidence during emergencies.

Theme 5: Protecting Guest Privacy While Implementing Security Strengthens Guest Confidence. Managers emphasized that stringent security measures must be accompanied by discretion and confidentiality. HM 5 described discreet security arrangements during celebrity arrivals, while HM 10 explained the quiet redirection of media personnel during VIP events to protect guest privacy. HM 15 similarly emphasized explaining CCTV monitoring as a safety and investigative measure rather than an invasion of privacy. These experiences demonstrate that privacy and security are complementary responsibilities, particularly in luxury hospitality where guests expect both protection and discretion.

The findings align with Karadayi-Usta (2024) and National Privacy Commission (NPC, 2023; 2024), which emphasize responsible information handling, access controls, confidentiality, accountability, and appropriate governance of surveillance systems. They also support the DICT/PNP (2024) and CICC (2025) emphasis on protecting personal and digital information amid evolving security threats. Overall, the theme demonstrates that privacy-conscious security practices strengthen guest trust by protecting personal dignity and confidentiality while maintaining necessary safeguards.

Taken together, Themes 3–5 demonstrate that effective luxury hotel security is characterized by **discreet enforcement, calm and coordinated emergency response, and strong privacy protection**. The managers' experiences show that security becomes more effective when technical and procedural safeguards are supported by professional judgment, communication, teamwork, and sensitivity to guest needs. These findings reinforce the broader conclusion that security and hospitality can operate as complementary objectives when security measures are implemented with competence, discretion, and a guest-centered approach.

Synthesis of the Themes. The five themes collectively demonstrate that balancing hospitality and security in luxury hotels requires a **guest-centered approach to security implementation**. Rather than treating security and hospitality as competing priorities, the managers' experiences show that they can be integrated through respectful communication, consistent enforcement, discreet intervention, coordinated emergency response, and protection of guest privacy. Across the narratives, the manner in which security measures are implemented emerged as equally important as the measures themselves.

Respectful communication and professionalism formed the foundation for guest cooperation, while consistent identity verification and access control ensured that security procedures were applied fairly without compromising service. Discreet enforcement further minimized disruption to the guest experience, whereas calm and coordinated emergency responses strengthened perceptions of safety and confidence during critical incidents. At the same time, protecting guest privacy through confidentiality and discretion reinforced trust, particularly among guests requiring heightened security.



Taken together, the findings indicate that effective hotel security extends beyond physical safeguards and operational procedures to include **interpersonal competence, ethical judgment, emotional intelligence, and service orientation**. Security was perceived not as a separate operational function but as an integral component of hospitality. By communicating respectfully, enforcing policies consistently, responding discreetly, coordinating effectively during emergencies, and safeguarding privacy, hotel managers create an environment in which guests feel both protected and welcomed. Thus, effective luxury hotel security depends on a holistic management approach that integrates operational security with exceptional guest service, thereby strengthening guest trust, confidence, and satisfaction.

Challenges in Balancing Guest Hospitality and Hotel Security. The qualitative findings showed that balancing hospitality and security in luxury hotels was a complex, people-centered process. Hotel managers had to protect guests, employees, and assets while maintaining the welcoming and personalized service expected in luxury establishments. Five interrelated themes emerged: (1) Managing Guest Resistance to Security Procedures, (2) Balancing Security Enforcement with a Welcoming Guest Experience, (3) Managing High-Stress Emergencies Without Creating Panic, (4) Balancing Security Verification with Guest Convenience, and (5) Protecting Guest Privacy While Maintaining Security. Collectively, these themes indicate that effective security depended not only on policies and technologies but also on communication, empathy, professionalism, discretion, and coordination.

Theme 1: Managing Guest Resistance to Security Procedures. Managers experienced occasional guest resistance to inspections, identity verification, visitor registration, and access controls, particularly when these procedures were perceived as inconvenient or intrusive. HM1 recalled handling VIP guests who questioned routine inspections and explained that calmly communicating the purpose and equal application of security policies encouraged cooperation. HM7 similarly noted that heightened security during large celebrations initially caused dissatisfaction, but guests became more receptive after the measures were explained. HM15 reported that visitor registration, emergency relocation, and security drills sometimes created inconvenience, which was reduced through timely updates and reassuring explanations.

These experiences suggest that resistance often resulted from inadequate understanding rather than opposition to security itself. This finding is consistent with Consortia Academia (2021), Torralba and Ylagan (2021), and Abad et al. (2025), who emphasized communication, professionalism, customer-service competence, and continuous training as important to effective hotel security. Thus, customer-oriented security training in communication, empathy, and conflict management may help personnel obtain cooperation without compromising security standards.

Theme 2: Balancing Security Enforcement with a Welcoming Guest Experience. Managers also faced the challenge of enforcing security policies without diminishing the guest experience. HM2 described situations involving unauthorized room access, intoxicated guests, and visitor registration during wedding celebrations, where firm enforcement had to be accompanied by courtesy. HM4 and HM10 similarly described discreet management of suspicious individuals, delivery personnel, media representatives, and VIP events to protect guests without unnecessarily disrupting hotel operations. HM14 noted that restrictions on photography and access to sensitive areas were more readily accepted when explained respectfully.

The findings demonstrate that effective enforcement requires operational authority to be combined with professionalism, discretion, and empathy. This supports Nagaj and Žuromskaite (2020), Hernandez-Calderon (2021), Torralba and Ylagan (2021), and Consortia Academia (2021), who emphasized that security measures can enhance guest confidence when they are integrated into hotel operations without unnecessarily disrupting service. The findings further support Abad et al. (2025) and Sisneros et al. (2025), who highlighted the importance of combining technical security knowledge with customer-service and judgment skills.

Theme 3: Managing High-Stress Emergencies Without Creating Panic. Emergency situations presented a distinct challenge because managers had to act quickly while maintaining guest confidence. HM3 described responding to suspicious packages, evacuations, and a missing child incident while keeping guests calm. HM9 similarly recalled medical emergencies and bomb threats that required organized evacuation, continuous communication, and calm leadership. HM12 reported coordinating a missing-child response and gas-leak evacuation while providing reassurance to affected guests.

These accounts show that emergency management requires both operational competence and emotional leadership. The findings support Algario et al. (2024), Abad et al. (2025), and Sisneros et al. (2025), who emphasized preparedness, interdepartmental coordination, continuous training, and organizational readiness. They also correspond with incident-response principles discussed by Mandiant (2024, 2025) and CrowdStrike (2025), particularly the importance of rapid detection, coordinated action, communication, and rehearsed procedures. Accordingly, emergency preparedness programs should integrate crisis communication, leadership, evacuation management, and interdepartmental coordination.

Theme 4: Balancing Security Verification with Guest Convenience. Identity verification, visitor registration, and access control were viewed as essential but could cause delays, particularly during peak periods. HM1 emphasized the need to complete verification thoroughly without creating excessive waiting time. HM6 described tour group and conference arrivals in which coordination among departments helped accelerate processing while maintaining required checks. HM11 similarly reported delays during conference badge verification, which were better received when procedures were clearly explained. HM15 noted that timely communication and courteous service helped minimize dissatisfaction during busy periods.



These findings indicate that security effectiveness is closely connected to operational efficiency. They support Qiu (2023), who emphasized usability, efficiency, and privacy in the acceptance of contactless hotel technologies, as well as Tourism Management (2020) and Consortia Academia (2021), which linked guest perceptions of safety with consistent and unobtrusive security practices. Abad et al. (2025) and Sisneros et al. (2025) further emphasized staff preparedness and coordination. Hotels may therefore benefit from streamlined verification processes, appropriate technological solutions, and stronger interdepartmental coordination.

Theme 5: Protecting Guest Privacy While Maintaining Security. Privacy protection emerged as an important challenge because luxury guests expect confidentiality alongside physical safety. HM4 and HM10 described discreet management of celebrity guests and media representatives, while HM11 recalled concerns about CCTV surveillance. Explaining that surveillance was intended for safety, crime prevention, and incident investigation helped address these concerns. HM14 similarly reported that restrictions on photography in sensitive areas were more acceptable when their security and privacy purposes were explained.

The findings suggest that privacy governance is an integral component of contemporary hotel security. This is consistent with Karadayi-Usta (2024) and Qiu (2023), who emphasized responsible security governance, usability, and privacy in technology-supported hotel operations. Torralba and Ylagan (2021) likewise stressed the importance of personnel competence and ethical service delivery. The findings therefore support strengthening privacy policies, confidentiality training, transparent communication about surveillance, and discreet security practices.

Synthesis of the Themes. The five themes collectively demonstrate that balancing hospitality and security in luxury hotels is fundamentally a process of sustaining guest trust. Guest resistance, security enforcement, emergency response, identity verification, and privacy protection all require more than procedural compliance; they demand professionalism, empathy, clear communication, discretion, and coordinated action.

Across the managers' experiences, security was most effectively integrated into hospitality when procedures were explained respectfully, enforced consistently, implemented discreetly, and supported by efficient service and calm leadership. Emergency situations further demonstrated the importance of coordination and reassurance, while privacy concerns highlighted the need for ethical and transparent security practices.

Overall, the findings indicate that effective luxury hotel security is achieved through the integration of people, processes, and technology. Hotel managers and security personnel function not only as protectors of guests, employees, and assets but also as representatives of the hotel's service culture. When security measures are implemented with professionalism and guest-centered communication, hotels can maintain strong protection while preserving guest comfort, confidence, and trust.

Influence of Experience on the Management of Hospitality and Security. The participants' experiences significantly influenced how they managed the relationship between hospitality and security. Rather than simply reinforcing existing practices, these experiences prompted improvements in communication, operational efficiency, emergency preparedness, security enforcement, and privacy protection. Five interrelated themes emerged: (1) Improving Communication to Encourage Guest Cooperation, (2) Balancing Efficient Service with Security Procedures, (3) Strengthening Emergency Response Through Better Coordination and Communication, (4) Strengthening Security Procedures While Maintaining Hospitality, and (5) Enhancing Guest Trust Through Privacy Protection and Professional Security Practices. Collectively, the themes demonstrate how practical experiences shaped managerial decisions and encouraged continuous improvement in both guest service and security operations.

Theme 1: Improving Communication to Encourage Guest Cooperation. The participants learned that respectful communication, empathy, and transparency were essential to gaining guest cooperation. HM1 emphasized that explaining the purpose of inspections and identity verification was as important as enforcing the procedures. HM2 similarly observed that guests were more cooperative when access controls and restrictions were implemented calmly and respectfully. HM5, HM7, HM10, HM12, and HM15 likewise highlighted timely updates, clear explanations, and professional communication as effective means of reducing resistance and maintaining a welcoming atmosphere.

These experiences indicate that communication functions as a bridge between security and hospitality. This finding supports Hernandez-Calderon (2021), Tourism Management (2020), and MDPI Sustainability (2023), which associated clear communication with greater guest acceptance of safety measures. It also corroborates Torralba and Ylagan (2021), Bartolome (2023), Abad et al. (2025), and Sisneros et al. (2025), who emphasized communication, professionalism, customer-service competence, and continuous training in effective hotel security. Thus, communication should be treated as a core security competency alongside technical skills.

Theme 2: Balancing Efficient Service with Security Procedures. The participants' experiences also encouraged them to improve operational efficiency without compromising security requirements. HM1 emphasized the need to complete identity verification while keeping service efficient. HM6 reported that stronger coordination among departments facilitated faster check-ins and event registration without omitting required verification. HM10, HM11, and HM15 similarly described improvements in planning and coordination that reduced delays while preserving access-control procedures.

The findings demonstrate that security and service efficiency can be pursued simultaneously through effective planning, streamlined processes, and interdepartmental coordination. This supports Qiu (2023), who emphasized convenience and usability in the



acceptance of security technologies, as well as Nagaj and Žuromskaite (2020) and Karadayi-Usta (2024), who highlighted operational efficiency and coordinated security management. Local studies by Torralba and Ylagan (2021), Bartolome (2023), and Consortia Academia (2021) likewise support the integration of personnel, procedures, and service quality. Hotels may therefore benefit from process improvements, integrated systems, and coordinated workflows that minimize inconvenience without weakening security.

Theme 3: Strengthening Emergency Response Through Better Coordination and Communication. Experiences with emergencies strengthened managers' emphasis on preparedness, teamwork, and communication. HM3 learned the importance of calm instructions and rapid coordination during medical emergencies and evacuations. HM5 emphasized timely updates to maintain guest confidence, while HM8 and HM13 reported that stronger teamwork improved investigations and emergency responses. HM15 likewise noted that better planning, communication, and coordination strengthened evacuation procedures.

These experiences demonstrate that emergency preparedness involves more than technical procedures; it also requires calm leadership and effective communication. The findings support Felicen et al. (2020), Algario et al. (2024), Abad et al. (2025), and Sisneros et al. (2025), who emphasized drills, organizational readiness, interdepartmental coordination, and continuous training. They are also consistent with Hernandez-Calderon (2021), UNLV (2021), Pipyros and Liasidou (2025), CrowdStrike (2025), and Mandiant (2024, 2025), which underscore communication, coordination, preparedness, and timely decision-making in crisis response. Regular multidisciplinary emergency simulations should therefore include not only technical response procedures but also communication, leadership, teamwork, and guest reassurance.

Theme 4: Strengthening Security Procedures While Maintaining Hospitality. The participants also reported that their experiences encouraged them to strengthen security procedures while keeping hospitality at the center of operations. HM2 learned that consistent enforcement was more effective when combined with empathy. HM4 described making security arrangements for VIP guests and restricted areas more discreet, while HM7 and HM12 reported improvements in crowd management and access control. HM11 similarly noted that better coordination strengthened verification procedures without compromising guest service.

These accounts demonstrate a shift toward integrated security management in which stronger controls support rather than undermine hospitality. The findings are consistent with Nagaj and Žuromskaite (2020), Tourism Management (2020), Karadayi-Usta (2024), Pipyros and Liasidou (2025), Torralba and Ylagan (2021), Bartolome (2023), Abad et al. (2025), and Sisneros et al. (2025), which emphasize professionalism, coordinated procedures, adaptability, and continuous staff development. Regular review of security procedures and customer-service-oriented training may therefore help hotels maintain rigorous controls while preserving guest comfort.

Theme 5: Enhancing Guest Trust Through Privacy Protection and Professional Security Practices. The participants' experiences also reinforced the importance of privacy and professional conduct. HM4 and HM5 emphasized discreet handling of VIP guests and sensitive situations, while HM9 described more careful ownership verification, room security, and media coordination. HM14 similarly reported strengthened procedures for protecting guest rooms, property, and confidentiality.

These experiences indicate that privacy protection is both a security responsibility and a dimension of luxury hospitality. The findings support Karadayi-Usta (2024) and Qiu (2023), who emphasized privacy, responsible security governance, and user acceptance of security technologies. They also align with Hernandez-Calderon (2021), the National Privacy Commission (2023, 2024), Bartolome (2023), and Torralba and Ylagan (2021), which stress transparency, confidentiality, accountability, and professional conduct. Hotels should therefore strengthen privacy policies, confidentiality training, ethical information handling, and transparent communication about surveillance and other security practices.

Synthesis of the Themes. The five themes demonstrate that managers' experiences reshaped their approach to hospitality and security by moving beyond strict policy enforcement toward a more integrated, guest-centered model. Across the themes, communication emerged as the central mechanism for gaining cooperation, managing emergencies, explaining security requirements, and addressing privacy concerns. Respectful explanations, empathy, transparency, and timely information helped transform potentially intrusive security measures into practices that guests could understand and accept.

The findings also emphasize operational integration. Experiences with identity verification, crowd management, emergencies, and access control encouraged managers to improve planning, interdepartmental coordination, and service efficiency rather than compromise security requirements. At the same time, professionalism, discretion, and ethical conduct enabled managers to strengthen security while protecting guest comfort, dignity, confidentiality, and trust.

Overall, the experiences transformed security management into a process of continuous experiential learning and adaptation. The participants learned to integrate security procedures with communication, efficient service, emergency preparedness, teamwork, and privacy protection. The overarching essence of the findings is that hospitality and security are not necessarily competing priorities; when managed through competent leadership and guest-centered practices, security becomes an extension of hospitality—protecting guests and hotel assets while strengthening confidence, comfort, and trust in the hotel experience.

Proposed Program to Enhance the Security Measures of the Target Hotels

The findings of the study revealed that although the selected luxury hotels have established comprehensive and effective security measures, hotel managers continue to encounter operational challenges in balancing guest hospitality with security requirements.



The qualitative findings showed that the greatest difficulties were not associated with the absence of security policies or procedures but with implementing these measures in ways that preserve the welcoming, personalized, and high-quality service expected in luxury hotels. Specifically, the participants experienced challenges in managing guest resistance to security procedures, enforcing security policies while maintaining a welcoming atmosphere, responding to emergencies without creating panic, conducting security verification without causing unnecessary delays, and protecting guest privacy while ensuring effective security operations.

These experiences indicate that the effectiveness of hotel security depends not only on physical safeguards, technology, and standard operating procedures but also on the competencies of hotel personnel in communication, professionalism, coordination, crisis management, and ethical decision-making. The findings further suggest that maintaining the delicate balance between hospitality and security requires continuous organizational learning and the enhancement of both technical and interpersonal skills.

In response to these challenges, a set of enhancement programs is proposed to further strengthen the security measures of the target hotels. These programs are designed to build upon the existing strengths of the hotels while addressing the practical issues identified by the participants. Anchored on the emergent themes of the qualitative findings, the proposed programs emphasize guest-centered communication, hospitality-oriented security practices, efficient security operations, emergency preparedness, and privacy protection. Collectively, these initiatives aim to sustain high standards of hotel security while reinforcing guest confidence, satisfaction, and trust, thereby supporting the long-term competitiveness and service excellence of the participating luxury hotels.

Luxury Hospitality Security Enhancement Program (LHSEP)

Goal: To continuously strengthen security management in the selected luxury hotels by enhancing communication, emergency preparedness, operational efficiency, guest privacy protection, and hospitality-oriented security practices while maintaining exceptional guest experiences.

Program Components

1. **Guest-Centered Security Communication Initiative.** It addresses Theme 1 and it focuses on communication, empathy, and conflict resolution.
2. **Hospitality-Security Integration Initiative.** It addresses Theme 2 and it develops customer-oriented security leadership and service excellence.
3. **Emergency Readiness and Crisis Management Initiative.** It addresses Theme 3 and it strengthens emergency coordination, drills, and crisis communication.
4. **Smart Guest Verification Initiative.** It addresses Theme 4 and it improves access control efficiency through technology and process optimization.
5. **Guest Privacy and Information Protection Initiative.** It addresses Theme 5 and it reinforces confidentiality, privacy governance, and ethical security practices.

Rationale

The proposed programs are directly grounded in the lived experiences of the hotel managers. The findings showed that the principal challenges were not the absence of security measures but the difficulty of implementing those measures while maintaining the standards of luxury hospitality. Specifically, managers encountered guest resistance to security procedures, operational delays during identity verification, challenges in handling emergencies without creating panic, the need to enforce security discreetly, and concerns about guest privacy. These experiences underscore that the effectiveness of hotel security depends as much on communication, professionalism, coordination, and ethical practice as on technical security controls.

Accordingly, the proposed programs emphasize capacity building, process improvement, technological support, and guest-centered security management. They are intended to strengthen existing security systems, sustain the high levels of implementation and effectiveness identified in the quantitative findings, and foster a culture in which hospitality and security are integrated rather than treated as competing priorities. This approach supports continuous organizational improvement while enhancing guest safety, confidence, and overall satisfaction.

Sustainable Mechanism for the Proposed Security Enhancement Programs

To ensure that the proposed security enhancement programs result in sustained improvements rather than one-time interventions, the selected luxury hotels should institutionalize a continuous improvement mechanism within their existing security and quality management systems. The mechanism should integrate organizational governance, staff development, performance monitoring, stakeholder feedback, technological review, and policy updating to ensure that security practices remain responsive to evolving risks and guest expectations.

A **Hotel Security and Hospitality Excellence Committee** should be established with representatives from management, security, front office, guest relations, housekeeping, engineering, human resources, and information technology. The committee should



oversee the implementation, monitoring, and periodic evaluation of security initiatives and ensure that security measures remain consistent with the hotel's service standards.

Continuous capacity building should be maintained through **semi-annual training and refresher programs** covering guest-centered security communication, emergency preparedness, privacy protection, crisis management, customer service, and conflict resolution. Scenario-based simulations, tabletop exercises, and after-action reviews should be incorporated to strengthen practical competence and organizational preparedness.

The hotels should also conduct an **annual review of security policies and procedures**, including Standard Operating Procedures, emergency response plans, privacy protocols, and access-control measures. Revisions should likewise be undertaken whenever significant changes occur in technology, legislation, hotel operations, or the threat environment.

Program performance should be monitored through measurable **Key Performance Indicators (KPIs)**, including compliance with security protocols, emergency response time, incident resolution time, security-related guest complaints, guest satisfaction with security services, and employee participation in training. Quarterly monitoring should be used to identify gaps and guide corrective actions.

Given the evolving nature of security threats, periodic assessment and upgrading of **security technologies and infrastructure** should be undertaken, including CCTV analytics, electronic access control, visitor management systems, cybersecurity controls, and emergency communication platforms. Technology adoption should improve security and operational efficiency without unnecessarily compromising guest convenience or privacy.

Guest participation should form part of the continuous improvement process through **security-related items in guest satisfaction surveys** and other feedback mechanisms. Guest perceptions of safety, concerns about privacy, and experiences with security procedures should be reviewed and used to improve policies and service delivery.

Regular **interdepartmental coordination meetings** should likewise be conducted to review incidents, emerging risks, operational challenges, and best practices. These should involve security and relevant operational departments to ensure that security responsibilities are understood as a shared organizational function.

Finally, **annual security audits, benchmarking, post-incident evaluations, and employee recognition mechanisms** should reinforce organizational learning and positive security behaviors. Lessons from audits and incidents should inform subsequent training, policy revisions, and operational improvements. Recognition of employees who demonstrate professionalism, ethical conduct, effective communication, crisis-management skills, and guest-centered security practices may further strengthen employee engagement and sustain a culture in which hospitality and security are treated as complementary responsibilities.

Monitoring and Evaluation Framework

The proposed programs should be monitored through the **Plan–Do–Check–Act (PDCA) Continuous Improvement Cycle**:

1. **Plan** – Identify emerging risks, guest concerns, operational gaps, and improvement priorities.
2. **Do** – Implement the recommended security and hospitality enhancement interventions.
3. **Check** – Assess implementation and outcomes through audits, KPIs, incident reports, training evaluations, and guest feedback.
4. **Act** – Revise policies, procedures, training, and operational practices based on evaluation results.

This cycle should be repeated regularly to ensure that security enhancement remains adaptive and responsive rather than a one-time activity.

Expected Long-Term Outcomes

The sustainable mechanism is expected to:

1. Institutionalize continuous improvement in hotel security management;
2. Strengthen personnel competencies in integrating hospitality and security;
3. Enhance guest trust, confidence, and satisfaction;
4. Improve preparedness for emerging physical, operational, and information-security threats;
5. Sustain high security standards without compromising luxury service; and
6. Strengthen organizational resilience through regular evaluation, innovation, and adaptation.

Overall, institutionalizing these mechanisms will integrate security enhancement into routine hotel governance and quality management. The proposed approach will help ensure that security practices remain **continuous, measurable, adaptive, and sustainable**, while preserving the personalized and high-quality hospitality expected of luxury hotels.

Conclusions

The following are concluded based on the findings of the study:



1. The selected luxury hotels demonstrated **full implementation** of personnel security, physical security, and document and information security measures, indicating consistent adherence to established security policies and procedures. The absence of significant differences among the hotels further suggests comparable levels of security implementation across the establishments.

2. The three security dimensions were likewise assessed as **highly effective**, with no significant differences in effectiveness among the selected hotels. These findings indicate that the participating establishments have achieved comparable levels of security performance in protecting guests, employees, assets, information, and hotel operations while maintaining quality hospitality services.

3. Significant positive relationships were found between security implementation and effectiveness across all three dimensions. The strength of these relationships indicates that more consistent implementation of security measures was associated with higher perceived security effectiveness. This finding underscores the importance of comprehensive and consistent execution of established security practices.

4. The qualitative findings further demonstrated that effective luxury hotel security extends beyond policies, procedures, and technological safeguards. Managers' experiences showed that balancing security with hospitality requires **guest-centered communication, professional and consistent enforcement, emergency preparedness, operational efficiency, coordinated action, and privacy protection**. Challenges involving guest resistance, service delays, emergencies, and privacy concerns encouraged managers to refine their practices and strengthen the integration of security and hospitality. Overall, the findings indicate that security and hospitality function as complementary dimensions of luxury hotel management when security measures are implemented with professionalism, empathy, discretion, and respect for guests.

5. Based on the integrated quantitative and qualitative findings, the **Luxury Hospitality Security Enhancement Program (LHSEP)** was proposed as a structured intervention to sustain existing strengths and address areas requiring continuous improvement. The program focuses on communication, emergency preparedness, operational efficiency, privacy protection, and hospitality-oriented security practices. Its implementation may help sustain effective security management while preserving the high-quality, guest-centered experience expected in luxury hospitality.

Recommendations

Based on the findings and the conclusions drawn, the following are hereby recommended:

1. **Sustain Established Security Practices.** Hotel management should sustain the full implementation of personnel, physical, and document and information security through regular policy reviews, periodic audits, continuous staff development, and timely adaptation to emerging threats.

2. **Strengthen Inter-Hotel Collaboration.** Since no significant differences were found in implementation across the selected luxury hotels, management should promote benchmarking, best-practice sharing, and joint security training to support continuous improvement and consistent security standards.

3. **Sustain Security Effectiveness.** Given the very high perceived effectiveness of the security measures, hotel administrators should continue investing in personnel competency, appropriate security technologies, preventive programs, and regular performance evaluation.

4. **Institutionalize Quality Monitoring.** Management should establish standardized security performance indicators and continuous quality-improvement mechanisms, supported by regular internal and external assessments, to maintain consistently high security outcomes.

5. **Ensure Consistent Implementation.** The significant positive relationship between implementation and effectiveness underscores the importance of consistent policy and procedure compliance. Management should therefore strengthen employee competency, resource allocation, technological support, and compliance monitoring.

6. **Strengthen Hospitality-Oriented Security.** Hotel management should enhance communication, customer service, emergency preparedness, operational coordination, and privacy protection through regular simulations, crisis communication workshops, guest-centered security training, and privacy awareness programs. Security awareness should extend across frontline and support departments to promote shared responsibility for guest safety.

7. **Implement and Evaluate the LHSEP.** The proposed **Luxury Hospitality Security Enhancement Program (LHSEP)** should be adopted as a comprehensive framework for strengthening communication, emergency response, operational efficiency, privacy governance, and intelligence-led security management. Its implementation should be supported by adequate resources, designated personnel, measurable indicators, and periodic monitoring and evaluation. Future researchers may assess the program after implementation and examine its applicability to other hospitality establishments, including boutique hotels, resorts, and business hotels.

REFERENCES

1. Abad, M., Jennifer, R., Grace, P., Jose, C., Gamboa, J. B., & Manuzon, E. P. (2025). *Safety and Security Practices of Hotels in Cabanatuan City: A Basis for Risk Management Plan*. *International Journal of Advanced Multidisciplinary Research and Studies*, 5(5), 133–141. <https://doi.org/10.62225/2583049x.2025.5.5.4869>
2. AHLA. (2025). *ENHANCED INDUSTRY-WIDE HOTEL CLEANING & SAFETY GUIDELINES*. https://www.ahla.com/sites/default/files/2025-11/2026_SafeStayGuidelines_AHLA.pdf



3. Arellano, J., Danica, L., Garcia, G. B., Iturralde, M. P., Mae, E., & Panganiban, M. P. (2024). *Level of Disaster Risk Preparedness of Selected Resorts in Talisay, Batangas*. *Journal of Business Innovation and Management*, 1(1), 1-1. <https://ejournals.ph/article.php?id=24353>
4. Bautista, P. S. (2024). Executive Order No. 58. *Lawphil.net*. https://lawphil.net/executive/execord/eo2024/eo_58_2024.html
5. Cruz, A. D. (2004). *The impact of security on Philippine tourism : a thesis presented in fulfilment of the requirements for the degree of Master of Philosophy in Development Studies at Massey University*. *Academia.edu*. https://www.academia.edu/83454870/The_impact_of_security_on_Philippine_tourism_athesis_presented_in_fulfilment_of_the_requirements_for_the_degree_of_Master_of_Philosophy_in_Development_Studies_at_Massey_University
6. Cyber Security Intelligence. (2026). Philippine National Police Anti-Cybercrime Group (PNP-ACG). *Www.cybersecurityintelligence.com*. <https://www.cybersecurityintelligence.com/philippine-national-police-anti-cybercrime-group-pnp-acg-4731.html>
7. Department of Information and Communications Technology (DICT). (2024). *National Cybersecurity Plan 2023-2028*. <https://Cms-Cdn.e.gov.ph>. <https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf>
8. Department of Tourism. (2020). *HEALTH AND SAFETY GUIDELINES GOVERNING THE OPERATIONS OF ACCOMMODATION ESTABLISHMENTS UNDER THE NEW NORMAL*. <https://Mail.hrap.org.ph>. https://mail.hrap.org.ph/advisory/advisory_2020-022_dot_memo2020-002.pdf
9. Department of Tourism. (2021). *ADMINISTRATIVE ORDER NO. 2021-UPDATED GUIDELINES ON THE OPERATIONS OF HOTELS AND OTHER ACCOMMODATION ESTABLISHMENTS UNDER A COMMUNITY QUARANTINE*. <https://law.upd.edu.ph/wp-content/uploads/2022/06/DOT-Administrative-Order-No-2021-004.pdf>
10. Department of Tourism. (2023a). *Home - Be part of the fun! Welcome to the DOT Corporate Site*. *Be Part of the Fun! Welcome to the DOT Corporate Site*. <https://beta.tourism.gov.ph>
11. Department of Tourism. (2023b). *THE NATIONAL TOURISM DEVELOPMENT PLAN 2023-2028 Approved Final Report*. <https://www.visitcentralluzon.com/wp-content/uploads/2026/02/DOT-NTDP-23-00043-Department-of-Tourism-National-Tourism-Development-Plan-2023-2028.pdf>
12. ENISA. (2024, October). *ENISA Threat Landscape 2024*. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
13. Finley Firm. (2024, February 6). *How poor hotel security procedures can lead to thefts, assaults*. *The Finley Firm, P.C. |; The Finley Firm, P.C.* <https://www.thefinleyfirm.com/blog/2024/02/how-poor-hotel-security-procedures-can-lead-to-thefts-assaults/>
14. Gatchalian, C. R. (2025, January 31). *CICC records over 10,000 cybercrime complaints in 2024 | ABS-CBNNews*. ABS-CBN. <https://www.abs-cbn.com/news/technology/2025/1/31/cicc-records-over-10-000-cybercrime-complaints-in-2024-1628>
15. Hicap, J. (2024, October 30). *Man who stole from guests at luxury hotels in Taguig, Makati arrested*. *Manila Bulletin*. <https://mb.com.ph/2024/10/30/man-who-stole-from-guests-at-luxury-hotels-in-taguig-makati-arrested>
16. Hunter, K. (2022, April 12). *Asylum seeker made 72 calls before hotel stabbings*. *BBC*. <https://www.bbc.com/news/uk-scotland-61073494>
17. International Organization for Standardization. (2019). *Paints and varnishes – Determination of solarreflectance*. ISO. <https://www.iso.org/standard/74252.html>
18. International Organization for Standardization. (2021). *Travel risk management Guidance for organizations*. ISO. <https://www.iso.org/standard/54204.html>
19. International Organization for Standardization. (2022). *ISO/IEC 27001 standard – information security management systems*. ISO. <https://www.iso.org/standard/27001>
20. Kurata, Y. B., Ong, A. K. S., Prasetyo, Y. T., Dizon, R. M., Persada, S. F., & Nadlifatin, R. (2023). *Determining factors affecting perceived effectiveness among Filipinos for fire prevention preparedness in the National Capital Region, Philippines: Integrating Protection Motivation Theory and extended Theory of Planned Behavior*. *International Journal of Disaster Risk Reduction*, 85(103497), 103497. <https://doi.org/10.1016/j.ijdr.2022.103497>
21. Marino, J., Roberts, G., & Moore, T. (2024, November 30). *Burglar steals safe containing \$400K after breaking into luxe NYC apartment*. *New York Post*. <https://nypost.com/2024/11/30/us-news/burglar-steals-money-and-baubles-from-posh-uws-pad/>
22. Nagaj, R., & Žuromskaitė, B. (2020). *Security Measures as a Factor in the Competitiveness of Accommodation Facilities*. *Journal of Risk and Financial Management*, 13(5), 99. <https://doi.org/10.3390/jrfm13050099>
23. National Disaster Risk Reduction and Management Council. (2019). *National disaster risk reduction and management plan 2020–2030*. *Ndrmc.gov.ph*. <https://ndrrmc.gov.ph>
24. National Privacy Commission. (2020). *GUIDELINES ON THE USE OF CLOSED-CIRCUIT TELEVISION (CCTV) SYSTEMS*. In *ResearchGate*. <https://privacy.gov.ph/wp-content/uploads/2020/11/Advisory-on-CCTV-16NOV2020-FINAL.pdf>
25. Noelah, M., & Borbon. (2020). *Evaluation on Disaster Preparedness among Resort Employees in Coastal Area situated in Batangas, Philippines*. <https://research.lpubatangas.edu.ph/wp-content/uploads/2020/08/Evaluation-on-Disaster-Preparedness-among-Resort-Employees-in-Coastal-Area-situated-in-Batangas-Philippines.pdf>
26. Obagha, B. B., Onen, O. P., Omubo, R. F., & Eyo, E. E. (2026). *Hotel Security Preparedness and Vulnerability to Armed Robbery and Kidnapping in Cross River State, Nigeria*. 1(1). <https://doi.org/10.60787/johrms.vol1no1.28>
27. PCI Security Standards Council. (2024). *PCI Data Security Standard (PCI DSS)*. PCI Security Standards Council. <https://www.pcisecuritystandards.org/standards/pci-dss/>



28. Rawlinson, K. (2026, March 30). Sexual assault survivor calls failure of Travelodge boss to meet MPs "shocking." *The Guardian*; *The Guardian*. <https://www.theguardian.com/society/2026/mar/30/sexual-assault-survivor-calls-failure-travelodge-boss-meet-mps-shocking>
29. Republic of the Philippines. (2021). Safety Seal Certification Program. <http://safetyseal.dti.gov.ph/>
30. Rita. (2024, October 30). Man linked to several hotel thefts arrested in Makati. *GMA News Online*. <https://www.gmanetwork.com/news/topstories/metro/925440/man-linked-to-several-hotel-thefts-arrested-in-makati/story/>
31. Rocamora, J. A. L. (2021). Makati hotel ordered to explain possible GCQ violation. <https://www.pna.gov.ph.https://www.pna.gov.ph/articles/1126352>
32. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *NIST Special Publication 800-207*, 1(800-207). <https://doi.org/10.6028/nist.sp.800-207>
33. Savita, R., & Singh, V. (2024). A systematic review on structure of hotel safety and security service: dimensions and measures A SYSTEMATIC REVIEW ON STRUCTURE OF HOTEL SAFETY AND SECURITY SERVICE: DIMENSIONS AND MEASURES. *Academy of Marketing Studies Journal*, 28(S5), 1–21. <https://www.abacademies.org/articles/a-systematic-review-on-structure-of-hotel-safety-and-security-services-dimensions-and-measures.pdf>
34. Savita, Rana, V., & Singh, S. (2024). A SYSTEMATIC REVIEW ON STRUCTURE OF HOTEL SAFETY AND SECURITY SERVICE: DIMENSIONS AND MEASURES. *Academy of Marketing Studies Journal*, 28(S5), 1–21. https://www.researchgate.net/publication/383952955_A_SYSTEMATIC_REVIEW_ON_STRUCTURE_OF_HOTEL_SAFETY_AND_SECURITY_SERVICE_DIMENSIONS_AND_MEASURES
35. Sisneros, R., Abrau, C. F. R., Tuto, A., & Olivar, K. (2025). An evaluation of safety preparedness and security measures of hotels in Davao city after Covid-19 pandemic. <https://doi.org/10.22271/27069583.2025.v7.i2a.165>
36. Torralba, M. A., & Ylagan, A. D. (2021). Safety and Security among Resorts in Batangas Province.9(2),80–88. https://www.researchgate.net/publication/381737838_Safety_and_Security_among_Resorts_in_Batangas_Province
37. U.S. Department of Defense. (2017). Department of Defense Annual Report on Sexual Assault in the Military Fiscal Year 2015. Createspace Independent Publishing Platform.
38. UNWTO . (2020). UNWTO Launches Global Guidelines to Restart Tourism | UN Tourism. [Untourism.int.https://www.untourism.int/news/unwto-launches-global-guidelines-to-restart-tourism](https://www.untourism.int/news/unwto-launches-global-guidelines-to-restart-tourism)
39. Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Enterprise Solutions. <https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf>
40. Verma, S. (2025, July 22). Washroom Heist: Luxury Fittings Worth Rs 35 lakh Stolen From 5-Star Hotel In Kolkata. *News18*. <https://www.news18.com/india/washroom-heist-luxury-fittings-worth-rs-35-lakh-stolen-from-5-star-hotel-in-kolkata-ws-l-9455954.html>
41. World Travel & Tourism Council. (2025). World Travel & Tourism Council (WTTC) | Travel & Tourism. [Wttc.org.https://wttc.org](https://wttc.org)
42. WTTC. (2020, May 27). WTTC launches world's first ever global safety stamp to recognise "Safe Travels" protocols around the world. [Wttc.org; World Travel & Tourism Council.https://wttc.org/news/wttc-launches-global-safety-stamp-to-recognise-safe-travels-protocols-around-the-world](https://wttc.org/news/wttc-launches-global-safety-stamp-to-recognise-safe-travels-protocols-around-the-world)