Journal of Hospitality and Tourism Management

Effect of Types of Access Control Systems on Data Protection Compliance and Security in Star-Rated Hotels in Nairobi

Hussein Bare Aden, Eric Bor & Samwel Auya

ISSN: 2706-6592

Stratford Peer Reviewed Journals and Book Publishing
Journal of Hospitality and Tourism Management
Volume 9||Issue 2||Page 26-40/August||2026
Email: info@stratfordjournals.org ISSN: 2706-6592

Effect of Types of Access Control Systems on Data Protection Compliance and Security in Star-Rated Hotels in Nairobi

[*1]Hussein Bare Aden, [2]Eric Bor & [3]Samwel Auya

[1]Department of Peace, Security and Social Studies, Egerton University, Kenya

[2]Faculty of Arts and Social Sciences, Department of Peace, Security, and Social Studies, Egerton University, Njoro, Kenya

Email Address: erick.bor@egerton.ac.ke

[3]Faculty of Arts and Social Sciences, Department of Peace, Security, and Social Studies, Egerton University, Njoro, Kenya

Email Address: samwel.auya@egerton.ac.ke

***Email of the Corresponding Author:** BARE.0035213@student.egerton.ac.ke

How to cite this article: **Aden, B., H., Bor, E. & Auya, E. (2026). Effect of Types of Access Control Systems on Data Protec-tion Compliance and Security in Star-Rated Hotels in Nairobi.** ***Journal of Hospitality & Tourism Management*** **9(2), 26-40. https://doi.org/10.53819/81018102t3184**

Abstract

Star-rated hotels in Nairobi manage extensive sensitive guest data, making them prime targets for cyberattacks. This study examined the relationship between types of access control systems and data protection compliance in star-rated hotels in Nairobi, Kenya. Guided by the Deterrence Theory of Information Security, the study adopted a mixed-methods embedded design. A census of all 60 star-rated hotels was conducted. Four respondents per hotel were targeted (one Hotel Manager, one IT professional, one front desk staff member, and one Security Officer), yielding a target population of 240 respondents. A total of 215 (89.6%) completed and returned the questionnaire. Data were collected via structured questionnaires and interviews. Regression analysis was conducted at a 0.05 significance level using SPSS. Results showed that types of access control systems had a significant positive effect on compliance ($R = 0.452$, $R^2 = 0.204$, $p < 0.05$), leading to rejection of the null hypothesis. The study concludes that the types of access control systems implemented have a statistically significant positive effect on data protection compliance. The Office of the Data Protection Commissioner should develop sector-specific guidelines for hospitality establishments that translate the Kenya Data Protection Act (2019) into actionable access control standards.

Keywords: *Access Control Systems, Data Protection Compliance, Star-Rated Hotels, Nairobi*

1.0 Background of the Study

The hospitality industry has undergone a significant transformation driven by the proliferation of digital technologies, necessitating robust security measures to protect sensitive data. Star-rated hotels, known for their high standards of service, cater to a diverse clientele, including high-profile individuals and corporate clients, making them prime targets for cyberattacks and data breaches (Wang, 2025). Globally, the hospitality industry has experienced numerous high-profile data breaches, underscoring the critical need for robust access control mechanisms. For instance, the Marriott International data breach in 2018 exposed the personal information of approximately 500 million guests, highlighting hotels' vulnerability to cyber threats (Marriott, 2018). Similarly, in 2014, the hotel group Mandarin Oriental experienced a data breach that compromised customer credit card information, underscoring vulnerabilities in their access control systems (Mandarin Oriental Hotel Group, 2015).

Access control mechanisms are fundamental in safeguarding sensitive data. Technologies such as biometric systems, Radio-Frequency Identification (RFID), and multi-factor authentication (MFA) have been implemented worldwide to enhance security. Biometric systems, such as fingerprint or facial recognition, are known for their high accuracy but raise privacy concerns and are expensive to implement (Mubarak et al., 2023). RFID, widely used for room access, offers convenience but is susceptible to cloning and interception (IBM X-Force Red, 2019a). MFA, which combines multiple verification methods, significantly reduces the risk of unauthorised access (Marriott International Inc., 2020). In the African context, the adoption of advanced access control systems is gaining momentum, though challenges remain. South Africa, for instance, has implemented the Protection of Personal Information Act (POPIA) to enforce data protection standards, urging hotels to enhance their data security measures (Pillay, 2018). However, many African countries face financial constraints and a lack of technical expertise, which hinders the implementation of sophisticated access control systems (Pillay, 2018).

In East Africa, the tourism sector is vital to the economy, necessitating stringent data protection practices. According to the World Travel & Tourism Council (WTTC), the tourism industry in Kenya, Tanzania, and Uganda is growing, with increasing international arrivals each year (WTTC, 2021). This growth amplifies the need for secure access control mechanisms to protect sensitive data and maintain global standards. Kenya's hospitality industry is a significant contributor to the country's economy, with Nairobi being a major business and tourism hub. The region hosts numerous star-rated hotels that cater to a diverse clientele, including business travellers, tourists, and international delegates. However, the industry's rapid growth has also attracted cybercriminals targeting sensitive guest information.

The Kenyan government has recognised the importance of data protection, leading to the enactment of the Data Protection Act in 2019. This legislation aligns with international standards, such as the General Data Protection Regulation (GDPR), and mandates stringent data protection measures, including effective access controls (Government of Kenya, 2019). Access control mechanisms are critical components of an organisation's security infrastructure, designed to regulate who can view or use resources in a computing environment. Inadequate or improperly implemented access controls can lead to unauthorised access to sensitive data, resulting in data breaches and financial losses. The complexity of managing access controls in star-rated hotels, which often operate multiple systems and networks, exacerbates the challenge (IBM X-Force Red, 2019a). Extensive research has been conducted on access control mechanisms and their role in data security across various industries. However, studies focusing specifically on the hospitality sector, and more so within the context of star-rated hotels in Nairobi, are limited.

Most existing literature addresses general cybersecurity measures and their application in broader contexts (Cylance Research Team, 2015).

Kenya's tourism industry, with Nairobi as a central hub, has seen significant growth, attracting leisure and business travellers. Star-rated hotels in Nairobi offer luxurious accommodations and advanced facilities, catering to an international clientele. The influx of digital technologies in hotel operations, ranging from online booking systems to digital payment platforms, has amplified the need for strong data security measures (Gwebu & Barrows, 2020). Despite technological advancements, implementing effective access control systems in Nairobi's star-rated hotels faces several challenges (Office of the Data Protection Commissioner, 2024). These include staff lack of awareness and training, financial constraints, and the complexity of integrating new technologies with existing systems (Njoroge, 2023). Additionally, regulatory frameworks and compliance requirements play a crucial role in shaping the security strategies adopted by these hotels. The Kenyan government has enacted several laws to enhance cybersecurity, including the Data Protection Act of 2019, which sets out requirements for data protection and the obligations of data controllers and processors (Government of Kenya, 2019). However, the enforcement and practical application of these regulations within the hospitality sector remain inconsistent. Many hotels in Nairobi continue to struggle with implementing effective access control systems due to financial constraints, limited technical expertise, and resistance to change.

Studies may offer general insights into access control systems, but there may be a gap in assessing their specific effectiveness in enhancing data protection compliance in the hospitality industry. The relationship between the technology used and its measurable outcomes in terms of security and compliance is often underexplored. Moreover, star-rated hotels may face unique security challenges due to their high profile, extensive guest services, and multiple access points. Therefore, there may be a gap in how access control systems are adapted to address these specific challenges, particularly in the context of Nairobi. In the rapidly evolving digital context, the hospitality industry, particularly star-rated hotels in Nairobi, faces significant challenges in safeguarding sensitive data whilst ensuring compliance with Kenya's Data Protection Act, 2019. The Communications Authority of Kenya reported over 3.4 billion cyber threat events in the 2023–2024 financial year, representing a fourfold increase from the previous year, with system vulnerabilities accounting for the majority of detected threats. The National KE-CIRT/CC issued over 27.5 million cyber threat advisories during the same period, highlighting the escalating risk to organisations handling sensitive data. Despite existing measures, many hotels experienced breaches resulting in financial losses, reputational damage, and legal consequences. Access control systems are critical in mitigating risks associated with data breaches and unauthorised access, yet many hotels struggle to implement effective mechanisms that balance security with operational efficiency. Despite the recognition of the importance of data protection, there is limited understanding of the specific types of access control systems in use and their effectiveness in securing sensitive information.

Additionally, challenges in adopting these systems often create gaps in data protection and regulatory compliance, exposing hotels to potential legal liabilities and reputational damage. This research examined the current state of access control systems in enhancing data protection and security compliance in star-rated hotels in Nairobi, assessed their effectiveness in protecting sensitive data, and identified the challenges hindering effective implementation. By addressing these issues, the study sought to contribute to the development of best practices to enhance data security and compliance in the hospitality sector.

2.0 Literature Review

Ashqar et al. (2023) studied access control in hotels in Portugal's Algarve region. They found that most hotels rely on Identity and Access Management (IAM) systems, which include multi-factor authentication, identity federation, and identity management software. However, their sample was only ten hotels in one region of Portugal, which limits generalisability. What works in the Algarve may not work in Nairobi due to different regulatory environments, threat landscapes, and hotel operations. This gap is addressed by the present study, which focuses on star-rated hotels in Kenya's capital. Akmese and Gundogan (2020) surveyed 120 hotel managers in five-star hotels in Alanya, Turkey. They examined whether managers' views on internal control systems varied based on duty segregation, asset protection, and transaction verification. Their results showed no significant difference across those variables. However, Turkey's hospitality regulations are not Kenya's, and their study used only questionnaires, with no interviews or site visits. This approach yields quantitative data but lacks depth. For Nairobi hotels, which must navigate the Data Protection Act, frequent cyber threats, and high staff turnover, surveys alone are insufficient. The present study uses mixed methods.

The National Cybersecurity Centre of Excellence (2021) emphasised the importance of access control systems in preventing unauthorised data access and ensuring data integrity. They highlighted the need for dynamic and adaptable access control policies that respond to evolving security threats. Esiefarienrhe and Ekka (2018) suggested role-based access control (RBAC) systems to enhance data security in organisational settings. In the hospitality industry, studies have shown that the transient nature of hotel staff and high turnover rates pose significant challenges to maintaining effective access controls (Shred-it, 2019). Integrating various systems, such as reservation, property management, and customer relationship management, requires a comprehensive approach to access control. Shanmugam et al. (2024) analysed technology-aided control systems in Malaysia's post-pandemic tourism industry. They discussed high-quality networks, stable Wi-Fi, and strong security protocols in five-star hotels. However, their focus was on guest experience and operational resilience, with data protection via access control as a secondary concern. Malaysia's infrastructure differs from Kenya's. A hotel manager in Nairobi, reading that study, would not learn how to handle a power outage that turns off card reader systems. The present study addresses this by examining Nairobi's actual conditions.

Medugu et al. (2023) studied security control systems in Lagos, Nigeria. They selected fifty hotels registered with Nigeria's National Tourism Development Corporation and interviewed security managers and other staff. They found that access control technologies increased efficiency, reliability, and security. However, Lagos is not Nairobi, and Nigeria's data protection law (NDPR) differs from Kenya's Data Protection Act of 2019. Their study focused on operational benefits rather than regulatory compliance, leaving it unclear how these systems help hotels pass a data protection audit. Prow and Company Advocates (2021) indicated that while many star-rated hotels in Nairobi have adopted basic access control measures, such as password-based systems and RFID cards, there is limited use of advanced technologies, such as biometrics and MFA. This gap leaves these establishments vulnerable to data breaches, as evidenced by several incidents reported in recent years.

Kimingi et al. (2024) conducted research in Nakuru County, Kenya, at 3- to 5-star hotels. They used a descriptive design, obtained 152 usable responses, and found a positive link between digital security systems and market performance. Access control systems emerged as the strongest factor. However, they measured "market performance", customer retention, and revenue, not regulatory compliance. A hotel can perform well in the market while still leaking

guest data. Nakuru also differs from Nairobi in hotel density, cyber threat volume, and regulatory attention. This study builds on Kimingi et al. by focusing specifically on data protection compliance in Nairobi's star-rated hotels and using a mixed-methods design. Access control systems regulate who can access resources in a computing environment. The primary types implemented in hotels include Biometric access systems that use physiological characteristics such as fingerprints, facial recognition, or iris scans for authentication. These systems offer high accuracy and are difficult to forge, but they raise privacy concerns and are costly to implement (Mubarak et al., 2023). Biometric data is classified as sensitive personal data under Kenya's Data Protection Act (2019), creating additional compliance obligations. Key card systems use magnetic stripe or RFID technology to grant access. They are widely used for guest room access in hotels. However, they are susceptible to cloning and interception (IBM X-Force Red, 2019a). Joseph Ng (2024) noted that while key cards are convenient, many hotels are transitioning to near-field communication (NFC) or mobile-based access solutions. Staff training on data protection and access control is a human-centric control that addresses employees' knowledge and behaviour. Solomon and Brown (2021) emphasised that organisational security culture and employee compliance behaviour are inextricably linked. Shred-it (2019) found that high turnover rates in hotels pose significant challenges to maintaining effective access controls.

Policy frameworks provide formal rules and procedures for managing access to personal data. These frameworks define roles, responsibilities, and accountability mechanisms. Gwebu and Barrows (2020) noted that hotels with comprehensive policies demonstrate stronger data protection practices. Physical security measures protect data storage areas through locks, surveillance cameras, and controlled entry points. These measures complement technical controls by preventing physical access to servers and data storage devices. Regulations play a crucial role in shaping access control practices. Kenya's Data Protection Act (2019) aligns with international standards, such as the General Data Protection Regulation (GDPR), and mandates stringent data protection measures, including robust access controls (Government of Kenya, 2019). The Act requires data controllers and processors to implement appropriate technical and organisational measures to ensure the security of personal data. International standards such as ISO/IEC 27001 provide frameworks for information security management. These standards recommend access control as a core component of information security. However, the enforcement and practical application of regulations within the hospitality sector remain inconsistent in Kenya. Many hotels struggle to implement effective access control systems due to financial constraints, limited technical expertise, and resistance to change (Njoroge, 2023).

2.1 Theoretical Framework

A theoretical framework establishes the underlying logic that connects variables in a study. The Deterrence Theory of Information Security guides this research. The theory explains how perceived costs, detection risk, and consequences shape compliance with security rules.

This theory posits that the threat of punishment can effectively prevent individuals and organisations from engaging in malicious activities that violate information security policies (Wang et al., 2019). It assumes people are rational decision-makers who weigh costs and benefits before taking action. By increasing the perceived costs of malicious activities, the threat of punishment can deter potential attackers, thereby reducing the likelihood of such incidents. Deterrence theory has its origins in criminology (Beccaria, 1764) and was formally applied to information security contexts by Straub (1990) and Straub and Welke (1998). The theory posits that the threat of punishment can effectively prevent individuals and organisations from engaging in malicious activities that violate information security policies (Wang et al., 2019). Gordon

and Loeb (2002) later applied economic principles to information security investment, suggesting that investments in security measures can raise the costs of attacks, thereby lowering the expected benefits for attackers.

Hotels implementing effective access control systems, such as role-based access control (RBAC), two-factor authentication (2FA), and encryption, can deter breaches and unauthorised access by raising the barriers for attackers and increasing the likelihood of detection (Maalem et al., 2020). This approach reduces the attractiveness of violating security measures and diminishes the risk of data compromise. The effectiveness of these controls was demonstrated by enhanced information security and fewer data breaches. Empirical evidence from studies conducted in star-rated hotels in the Greater Nairobi Region validated the application of the Deterrence Theory of Information Security in this context. The Deterrence Theory directly informs the four independent variables in this study. First, the types of access control systems (biometric, key card, training, policies, physical security) raise the perceived costs of unauthorised access, strengthening deterrence. Second, the effectiveness of access control systems, particularly monitoring and auditing features, increases the perceived certainty of detection – a core deterrence mechanism. Third, implementation challenges (e.g., regulatory complexity, maintenance costs) weaken deterrence by reducing the credibility and reliability of controls, which explains the hypothesised negative relationship. Fourth, ISO/IEC 27001-recommended strategies (e.g., stricter protocols, training, biometrics) enhance deterrence by closing vulnerabilities and increasing accountability.

2.2 Conceptual Framework

The conceptual framework (Figure 1) illustrates the hypothesised relationship between types of access control systems and data protection compliance in star-rated hotels in Nairobi.

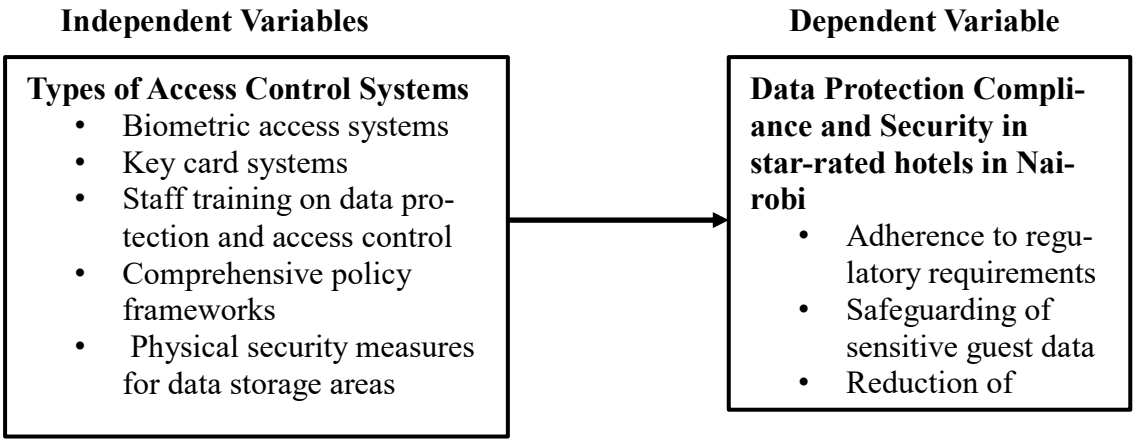

Figure 1:Conceptual Framework

The Deterrence Theory of Information Security informs the independent variable in this study. The types of access control systems (biometric, key card, training, policies, physical security) raise the perceived costs of unauthorised access, strengthening deterrence. The relationship is expected to be positive: hotels that implement a broader and more advanced range of access control systems achieve higher levels of data protection compliance.

3.0 Methodology

The study adopted a mixed-methods embedded design, with quantitative methods given priority and qualitative methods used to provide explanatory insights. A descriptive correlational approach was applied to examine the relationship between access control system types and

data protection compliance and security among star-rated hotels in the Greater Nairobi Region. The study targeted 60 hotels and purposively selected four respondents from each hotel, giving 240 respondents, of whom 215 participated, representing an 89.6% response rate. Data were collected using questionnaires and semi-structured interviews. Quantitative data were analysed using SPSS version 27 through descriptive statistics, Pearson correlation, and simple linear regression at a 0.05 significance level, while qualitative data were analysed thematically using NVivo 14 following Braun and Clarke's (2006) framework. Findings were presented using tables and figures.

4.0 Findings and Discussion

The questionnaire return rate for the study is presented in Table 2. The study targeted two hundred and forty (240) respondents from sixty (60) star-rated hotels in the Greater Nairobi Region, comprising Hotel Managers, IT personnel, front desk staff, and security officers. Of these, two hundred and fifteen (215) questionnaires were duly completed and returned, yielding a response rate of 89.6% (Table 2).

4.1 Descriptive Statistics

This section presents descriptive findings on the types of access control systems implemented by star-rated hotels in Nairobi to support data protection compliance and security, corresponding to the first study objective. Table 1 presents the distribution of responses on types of access control systems implemented. Responses were recorded on a five-point Likert scale from Strongly Disagree (1) to Strongly Agree (5).

Table 1: Distribution of Responses

Statement	SD(1)	D(2)	N(3)	A(4)	SA(5)	Mean	Std. Dev.
The hotels have implemented biometric access control systems for securing guest data.	2 (0.9%)	24 (11.2%)	91 (42.3%)	79 (36.7%)	19 (8.8%)	3.41	0.838
The hotel uses keycard systems to restrict access to sensitive areas and to guest data storage locations.	7 (3.3%)	46 (21.4%)	91 (42.3%)	59 (27.4%)	12 (5.6%)	3.11	0.913
Staff training on data protection and access control is regularly conducted.	0 (0.0%)	15 (7.0%)	80 (37.2%)	102 (47.4%)	18 (8.4%)	3.57	0.745
The hotel has a comprehensive policy for managing access to personal data.	3 (1.4%)	35 (16.3%)	99 (46.0%)	62 (28.8%)	16 (7.4%)	3.25	0.864
Physical security measures are in place to protect data storage areas.	3 (1.4%)	35 (16.3%)	95 (44.2%)	70 (32.6%)	12 (5.6%)	3.25	0.843

The frequency distribution shows that most respondents agreed or strongly agreed with most statements, indicating moderate to high levels of implementation of the access control system.

Staff training on data protection and access control recorded the highest combined positive response, with 47.4% agreeing and 8.4% strongly agreeing (55.8% total). In contrast, key card systems recorded the most mixed responses, with 24.7% disagreeing or strongly disagreeing. These results indicate that human-centred controls, such as training, were more consistently reported than technology-dependent controls, such as key card systems. The implication is that hotels should invest simultaneously in both technological and human capital dimensions of access control, rather than treating them as substitutes.

Table 2: Ranked Mean Scores

Rank	Statement	Mean Score
1	Staff training on data protection and access control is regularly conducted.	3.57
2	The hotels have implemented biometric access control systems for securing guest data.	3.41
3	The hotel has a comprehensive policy for managing access to personal data	3.25
4	Physical security measures are in place to protect data storage areas.	3.25
5	The hotel uses keycard systems to restrict access to sensitive areas and to guest data storage locations.	3.11

Staff training on data protection and access control received the highest mean score (M = 3.57, SD = 0.745). This implies that star-rated hotels in Nairobi invest more heavily in training than in technology. For a hotel manager, this suggests that staff behaviour is seen as the first line of defence, not access cards or biometrics. Biometric access control systems ranked second (M = 3.41, SD = 0.838). Biometrics are present but not universal. Four-- or five-star hotels without biometrics for server rooms are lagging behind their competitors. Both comprehensive policy frameworks and physical security measures scored M = 3.25. These findings suggest that policies exist on paper, but enforcement is inconsistent. Physical security for data storage areas is adequate but not excellent. Key card systems recorded the lowest mean (M = 3.11, SD = 0.913). Key cards are seen as outdated. Managers should plan a transition to near-field communication (NFC) or mobile-based access within 2 to 3 years.

To assess the level of agreement among respondents regarding the types of access control systems, Kendall's Coefficient of Concordance was computed. The results are summarised in Table 3.

Table 3: Kendall's Coefficient of Concordance for Types of Access Control Systems

Test Statistic	Value
N	215.0
Kendall's W	0.001
Chi-Square	0.693
df	4.0
Asymp. Sig.	0.952

a. Kendall's Coefficient of Concordance

The Kendall's W of 0.001 and Chi-square of 0.693 (df = 4, p = 0.952) indicated no statistically significant consensus among respondents in their ranking of the five access control system dimensions. The non-significant result ($p > 0.05$) suggested that respondents did not consistently rank the five types of access control systems in the same order, reflecting heterogeneity of access control priorities across different hotel categories and departments. This finding is consistent with Masaire et al. (2024), who found that information security priorities varied substantially across hotel types in developing country contexts, attributable to differences in resource endowment and operational focus.

4.3 Effect of Types of Access Control Systems on Data Protection Compliance and Security in Star-Rated Hotels in Nairobi

The study assessed the relationship between the types of access control systems implemented by star-rated hotels in Nairobi and data protection compliance and security. The null hypothesis tested was H_{01}: The types of access control systems implemented by star-rated hotels in Nairobi have no statistically significant effect on data protection compliance and security. Table 4 presents the bivariate Pearson correlation coefficient between the independent and dependent variables.

Table 4: Correlations with Data Protection Compliance

Variable	Pearson r	Sig. (2-tailed)
Types of Access Control Systems	0.452**	< 0.05

Types of access control systems recorded a statistically significant positive correlation ($r = 0.452$, $p < 0.05$). These findings provided preliminary evidence that types of access control systems are positively associated with data protection compliance, thereby justifying the subsequent simple linear regression analysis. The findings are consistent with Ghaderi et al. (2024), who identified system effectiveness as a primary cybersecurity determinant of compliance outcomes in hospitality contexts. A simple linear regression analysis was conducted with types of access control systems as the predictor variable and data protection compliance as the outcome variable. Table 5 presents the consolidated regression results.

Table 5: Linear Regression

Component	Statistic	Value
Model Fit	R	0.452
	R^2	0.204
	Adjusted R^2	0.196
	Std. Error of the Estimate	0.680
ANOVA	Regression Sum of Squares	25.265
	Regression df	1
	Regression Mean Square	25.265
	Residual Sum of Squares	98.581
	Residual df	213
	Residual Mean Square	0.463
	Total Sum of Squares	123.846
	Total df	214
	F	54.568
	Sig. (p)	0.000
Coefficients	(Constant)	
	Unstandardised B	1.245
	Std. Error	0.312
	t	3.990
	Sig. (p)	< 0.05
	Predictor (Types of ACS)	
	Unstandardised B	0.485
	Std. Error	0.065
	Standardised Beta	0.452
	t	7.387
	Sig. (p)	0.000

A linear regression model for access control system types yielded R = 0.452, indicating a moderate positive relationship between access control system types and data protection compliance. The R^2 of 0.204 indicated that types of access control systems explained 20.4% of the variance in data protection compliance and security. The adjusted R^2 of 0.196 confirmed this explanatory power after accounting for model complexity. The ANOVA results confirmed that the model was statistically significant: $F(1, 213) = 54.568$, $p = 0.000$. Since $p < 0.05$, the null hypothesis H_{01} was rejected. Types of access control systems implemented by star-rated hotels in Nairobi had a statistically significant positive effect on data protection compliance and security.

The following regression equation was specified:

$$Y = 1.245 + 0.485X_1 + \varepsilon$$

The constant was 1.245 (SE = 0.312; t = 3.990; $p < 0.05$). The unstandardised regression coefficient for types of access control systems was B = 0.485 (SE = 0.065; standardised $\beta = 0.452$; t = 7.387; p = 0.000). A one-unit increase in the composite mean score of the types of access control systems implemented was associated with a 0.485-unit increase in the mean score of data protection compliance. The implication is that hotels that implement a broader and more advanced suite of access control mechanisms achieve significantly higher levels of data protection compliance. Ashqar et al. (2023) demonstrated that diverse access control technologies strengthen data protection capabilities by creating multiple layers of security defence, consistent with this finding. Qualitative data from the semi-structured interviews, analysed thematically using NVivo 14 following Braun and Clarke's (2006) framework, identified three themes related to types of access control systems: predominant access control technologies in

use; staff training as the foundational security priority; and the gap between formal policy existence and practical enforcement.

Theme 1: Access Control Technologies in Use

Respondents consistently identified biometric systems, key card systems, and closed-circuit television integration as the primary access control technologies deployed in their hotels. IT managers and hotel managers from four- and five-star establishments described multi-layered implementations, whilst three-star hotel staff reported simpler configurations.

"We have biometric readers on all server rooms and main data storage areas. Staff access is role-based, and every entry is logged automatically." (IT Manager, Five-Star Hotel)

"*Our key card system covers guest rooms and restricted areas. We are currently evaluating biometric upgrades for the back-office systems*." (Hotel Manager, Four-Star Hotel)

"*We rely mainly on key cards and a password-based system for our front office computers. Biometrics are too expensive for us right now*." (Front Desk Supervisor, Three-Star Hotel)

These responses align with the quantitative finding that biometric systems (M = 3.41) were rated higher than key card systems (M = 3.11), with the gap reflecting resource differences between higher- and lower-star-rated establishments. Dijmărescu et al. (2022) observed that biometric integration is increasingly viewed as essential for payment and access security in modern hotel operations, consistent with the upward trend in biometric adoption observed among higher-rated establishments in this study.

Theme 2: Staff Training as the Foundational Security Priority

All respondents acknowledged that staff training was the most consistently implemented access control dimension, corroborating the quantitative result, which found that staff training received the highest mean score (M = 3.57).

"*We conduct mandatory quarterly training for all staff on data protection policies and proper use of the access control systems. Non-compliance is treated as a disciplinary matter*." (Human Resources Manager, Five-Star Hotel)

"*Training is conducted when new staff join and once a year as a refresher. We cover the Data Protection Act requirements and the proper use of our card access system*." (IT Personnel, Four-Star Hotel).

Solomon and Brown (2021) emphasised that organisational security culture and employee compliance behaviour are inextricably linked, which is consistent with the importance respondents attached to training as the foundational element of access control implementation.

Theme 3: The Gap Between Policy Existence and Practical Enforcement

Several respondents noted that whilst formal access control policies existed, practical enforcement was inconsistent, particularly in high-turnover front-of-house roles, providing a qualitative explanation for the comparatively lower mean score for policy frameworks (M = 3.25).

"*We have comprehensive policies on paper, but monitoring actual compliance in day-to-day operations is very difficult. Staff sometimes share passwords or leave terminals unlocked*." (IT Manager, Four-Star Hotel)

"*Policies are clear, but enforcement is where we struggle. There is a lot of pressure during busy periods, and security can take a back seat.*" (Hotel Manager, Three-Star Hotel).

This qualitative finding is consistent with Masaire et al. (2024), who found that the gap between formal information security policy and operational enforcement was a critical vulnerability in hotel-sector data protection frameworks in developing-country contexts.

5.0 Conclusions

The study sought to assess the relationship between the types of access control systems implemented by star-rated hotels in Nairobi and data protection compliance and security. The study concluded that the types of access control systems implemented in Nairobi's star-rated hotels had a statistically significant positive effect on data protection compliance. Hotels that deployed comprehensive access control portfolios encompassing biometric authentication, physical safeguards, staff training, and policy frameworks achieved higher compliance levels and better protection of sensitive data. However, the transition from traditional key card systems to advanced biometric solutions remains incomplete, suggesting a maturity gap in technological adoption. Staff training emerged as the most consistently implemented access control type, indicating that human-centred controls are prioritised over technology-dependent controls in the current hospitality environment.

6.0 Recommendations

The Office of the Data Protection Commissioner and Tourism Regulatory Authority should develop clear hospitality-specific data protection and cybersecurity standards for star-rated hotels. Hotel management should strengthen staff training, upgrade insecure access control technologies, and enforce clear data access policies and accountability mechanisms. Future studies should use longitudinal designs and conduct comparative research across East African countries to assess long-term effects and regional best practices.

References

Akmese, H., & Gundogan, R. (2020). The role of internal control systems in the hotel business: A case of five-star hotels in Alanya. *Journal of Business Research – Turk*, *12*(1), 123–135.

Ashqar, R. I., Ashqar, H. I., & Ramos, C. M. Q. (2023). Identity and access management in tourism and hospitality. In *Conference on Management, Tourism and Technology* (pp. 445–460). Springer. https://doi.org/10.1007/978-3-031-44131-8_32

Beccaria, C. (1764). *On crimes and punishments*. (Original work published 1764)

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Bryman, A., & Bell, E. (2015). *Business research methods* (4th ed.). Oxford University Press.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage Publications.

Cylance Research Team. (2015). Critical flaw in Wi-Fi routers puts hotels and millions of guests at risk. *Help Net Security*. https://www.helpnetsecurity.com/2015/03/27/critical-flaw-in-wifi-routers-puts-hotels-and-millions-of-guests-at-risk/

Dijmărescu, I., Iatagan, M., Hurloiu, I., Geamănu, M., & Dijmărescu, S. (2022). Neuromanagement decision-making in facial recognition biometric authentication as a mobile payment technology in retail, restaurant, and hotel business models. *Oeconomia Copernicana*, *13*(2), 509–540. https://doi.org/10.24136/oc.2022.019

Esiefarienrhe, B. M., & Ekka, A. H. (2018). Modified role-based access control model for data security. *International Journal of Scientific & Technology Research*, *7*(11), 182–186.

Ghaderi, Z., Beal, L., & Houanti, L. H. (2024). Cybersecurity threats in tourism and hospitality: Perspectives from tourists engaging with sharing economy services. *Current Issues in Tourism*, 1–22. https://doi.org/10.1080/13683500.2024.2353327

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457.

Government of Kenya. (2019). *Data Protection Act, No. 24 of 2019*. Kenya Gazette Supplement.

Gwebu, K., & Barrows, C. W. (2020). Data breaches in hospitality: Is the industry different? *Journal of Hospitality and Tourism Technology*, *11*(3), 511–527. https://doi.org/10.1108/JHTT-04-2019-0053

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2021). *Multivariate data analysis* (8th ed.). Cengage.

IBM X-Force Red. (2019a). Data leaks, default passwords exposed in visitor management systems. *ZDNet*. https://www.zdnet.com/article/data-leaks-default-passwords-exposed-in-visitor-management-systems/

Joseph Ng, P. S. (2024). Hotel room access control: An NFC approach to ecotourism framework. *Journal of Science and Technology Policy Management*, *15*(3), 530–548. https://doi.org/10.1108/JSTPM-06-2023-0095

Kimingi, A. M., Mwenda, L. K. M., & Chege, P. W. (2024). *Effect of digital security systems on market performance in 3–5 star rated hotels in Nakuru County, Kenya*. Dedan Kimathi University of Technology Repository.

Kothari, C. R. (2004). *Research methodology: Methods and techniques* (2nd ed.). New Age International.

Kundu, A., & Bej, T. (2021). Experiencing e-assessment during COVID-19: An analysis of Indian students' perception. *Higher Education Evaluation and Development*, *15*(2), 114–134.

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight into the behavioural aspects of cybersecurity. *Cybersecurity*, *3*(1), 1–18.

Mandarin Oriental Hotel Group. (2015, July 10). *Press release and notice regarding Mandarin Oriental credit card breach*. https://photos.mandarinoriental.com/is/content/MandarinOriental/corporate-global-pdf-mohg-malware-notice-july-10-2015

Marriott International Inc. (2020). Probing Marriott's mega-breach: 9 cybersecurity takeaways. *BankInfoSecurity*. https://www.bankinfosecurity.net/probing-marriotts-mega-breach-9-cybersecurity-takeaways-a-15338

Marriott. (2018, November 30). *Marriott announces Starwood guest reservation database security incident*. https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident

Masaire, T. M., Tsokota, T., & Chipfumbu, C. T. (2024). Information security in the Zimbabwean hotel sector. In *Tourism and hospitality for sustainable development* (pp. 87–108). Springer. https://doi.org/10.1007/978-3-031-63073-6_6

Medugu, J. D., Binuyo, B. A., Efunwole, A. A., & Oyebisi, S. O. (2023). Security control systems in the hospitality industry in Lagos Metropolis, Nigeria. *Journal of Hospitality and Tourism Insights*, *6*(3), 1122–1140.

Mubarak, R., Alsboui, T., Alshaikh, O., Inuwa-Dutse, I., Khan, S., & Parkinson, S. (2023). A survey on the detection and impacts of deepfakes in visual, audio, and textual formats. *IEEE Access*, *11*, 144497–144529. https://doi.org/10.1109/ACCESS.2023.3344653

Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods: Quantitative and qualitative approaches*. African Centre for Technology Studies.

National Cybersecurity Centre of Excellence. (2021). *Securing property management systems* (NIST SP 1800-27). National Institute of Standards and Technology. https://www.tripwire.com/state-of-security/nist-sp-1800-27-securing-property-management-systems

Nayak, M. S. D. P., & Narayan, K. A. (2019). Strengths and weaknesses of online surveys. *Technology*, *6*(7), 0837–2405053138.

Njoroge, J. (2023, October 10). Data protection is vital in the hospitality sector. *The Star (Kenya)*. https://www.the-star.co.ke/sports/football/2023-10-10-njoroge-data-protection-vital-in-hospitality-sector

Office of the Data Protection Commissioner. (2024). *Data Protection Compliance Directorate*. Government of Kenya. https://www.odpc.go.ke/data-protection-compliance/

Pillay, L. (2018). POPI: Changing the way SA tour operators do business. *Tourism Update*. https://www.tourismupdate.com/article/popi-changing-the-way-sa-tour-operators-do-business

Prow & Company Advocates. (2021). *Radisson Blu Hotel data breach complaint* (Complaint No. ODPC/COMP/2021/042). Office of the Data Protection Commissioner. https://caselawlibrary.cipit.org/complaints/detail/radisson-blu-data-breach

Shanmugam, M., Rana, N. P., & Kong, X. (2024). Technological advancements and smart tourism strategies in Malaysia's post-pandemic tourism industry. *Journal of Smart Tourism*, *5*(1), 33–50.

Shred-it. (2019). *2019 data protection report: Hospitality findings*. https://www.shredit.com/en-ca/blog/protect-hotel-guests-confidential-information

Simon, M. K., & Goes, J. (2012). *Dissertation and scholarly research: Recipes for success* (2nd ed.). CreateSpace Independent Publishing Platform.

Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management*, *35*(4/5), 1024–1047. https://doi.org/10.1108/JEIM-08-2019-0217

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255–276.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision-making. *MIS Quarterly*, *22*(4), 441–469.

Tourism Regulatory Authority. (2023). *Register of classified establishments for the period 2015–2023 in Kenya by TRA classification regions*. https://tra.go.ke/classification-and-grading/

Wang, J., Shan, Z., Gupta, M., & Rao, H. R. (2019). A longitudinal study of unauthorised access attempts on information systems: The role of opportunity contexts. *MIS Quarterly*, *43*(2), 601–622.

Wang, T. (2025). Has your information been leaked? The impact of cybersecurity risks on the performance of tourism enterprises. *Current Issues in Tourism*, 1–20. https://doi.org/10.1080/13683500.2025.2501678

World Travel & Tourism Council. (2021). *Kenya's tourism numbers up by 40%*. Tourism Update. https://www.tourismupdate.com/article/kenyas-tourism-numbers-up-by-40

Yang, S., & Berdine, G. (2021). Normality tests. *The Southwest Respiratory and Critical Care Chronicles*, *9*(41), 50–52. https://doi.org/10.12746/swrccc2021.0901.222