International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Cybersecurity Controls Framework for Secure System and Network Access in the Hospitality Sector: A Case of Lake Victoria Hotel, Entebbe, Uganda

Musosi Elijah[1], Ali Najib[2], David Kaketo[3], Anthony Bua[4]

[1]Postgraduate Student, Faculty of Science and Technology, School of Postgraduate Studies and Research, Victoria University, Kampala, Uganda
[2,3]Senior Lecturer, Faculty of Science and Technology, School of Postgraduate Studies and Research, Victoria University, Kampala, Uganda
[4]Lecturer, Faculty of Science and Technology, School of Postgraduate Studies and Research, Victoria University, Kampala, Uganda

Abstract

Hotels across Uganda increasingly rely on networked systems for reservations, payments, and guest services, yet many still operate without a structured, risk-based approach for protections, a gap that leaves properties such as Lake Victoria Hotel (LVH) in Entebbe exposed, as cyber threats facing the hospitality sector continue to grow. This study set out to close that gap by designing Cybersecurity Controls Framework (LVH-CCF) for secure system and network access, tailored to LVH's operational and regulatory environment.

This study was guided by three objectives: evaluating existing access control measures, including multi-factor authentication, role-based access control, privileged access management, and VLAN segmentation; developing an incident response and recovery plan aligned with NIST SP 800-61 Rev. 3; and finally, designing a controls framework anchored in NIST CSF 2.0, NIST SP 800-53 Rev. 5, Uganda's Data Protection and Privacy Act (DPPA) 2019, and the Computer Misuse (Amendment) Act (CMAA) 2022. The study is theoretically grounded in Systems Theory (Pigola et al., 2025), Protection Motivation Theory (Maalem Lahcen et al., 2020), and Compliance and Regulatory Theory.

The study used a mixed-methods case study design, drawing on structured surveys, semi-structured interviews, OpenVAS-assisted technical audits, and expert panel assessments across five respondent groups management, IT personnel, staff, external experts, and guests (N = 72). Quantitative data were analysed in SPSS using Wilcoxon Signed-Rank and Spearman correlation tests, while qualitative data were analysed thematically.

The findings painted a picture of a reactive, fragmented security posture. Basic perimeter defences were largely in place antivirus (100%), firewalls (86%), and backups (86%) but preventive and governance controls were almost entirely absent: no multi-factor authentication, a documented policy covering only 14% of respondents, network segmentation at just 14%, no staff training, and no incident response plan. Introducing a structured framework had a significant effect on secure system and network access (Wilcoxon W = 5.000, p = 0.0196), and access control measures showed a strong positive relationship

with system security (Spearman $\rho = 0.922$, $p < 0.001$) a result consistent with Protection Motivation Theory's prediction that behavioural security gains in one domain carry over into adjacent ones. The link between incident response preparedness and business continuity could not be statistically confirmed, given the small management sample ($n = 7$), though qualitative and cross-group evidence supported it.
The resulting LVH-CCF comprises 39 controls spanning the six NIST CSF 2.0 functions Govern (6), Identify (5), Protect (16), Detect (4), Respond (4), and Recover (4) sequenced across a five-phase roadmap. Implementing it would close LVH's most critical vulnerabilities, achieve verifiable DPPA 2019 compliance, and strengthen guest trust.

Keywords: Cybersecurity Controls Framework, NIST CSF 2.0, Access Control, Incident Response, Hospitality Industry, Data Protection and Privacy Act, Lake Victoria Hotel, Uganda.

Introduction

Hotels such as Lake Victoria Hotel (LVH) in Entebbe, Uganda, depends on a wide range of interconnected digital systems for reservations, payment processing, customer relationship management, and administrative operations. While these technologies improve operational efficiency and guest experience, they simultaneously expand the organisation's exposure to cyber threats including data breaches, ransomware, phishing, and unauthorised system access (Wynn & Lam, 2023). The consequences of inadequate cybersecurity in the hospitality sector can be severe: financial loss, reputational damage, loss of guest trust, and legal liability under Uganda's Data Protection and Privacy Act (The Republic of Uganda (Government), 2019) and the Computer Misuse (Amendment) Act (CMAA, 2022). Despite these risks, many hotels in developing countries continue to operate without structured, risk-based cybersecurity frameworks tailored to their specific operational and regulatory environments (Muhangi, 2019).
This study addressed this gap by designing and proposing a Cybersecurity Controls Framework for Secure System and Network Access at Lake Victoria Hotel, the LVH Cybersecurity Controls Framework (LVH-CCF). The framework is anchored in the NIST Cybersecurity Framework 2.0 (NIST CSF 2.0) and NIST SP 800-53 Rev. 5 and explicitly aligned to Uganda's DPPA 2019 and CMAA 2022. Through a mixed-methods case study encompassing structured surveys, semi-structured interviews, technical system audits, and expert panel assessments, the study produced an empirically grounded, locally compliant, and practically implementable framework comprising 39 controls distributed across the six NIST CSF 2.0 functions: Govern, Identify, Protect, Detect, Respond, and Recover (Pipyros & Liasidou, 2025).

Historical Perspective

Globally, hotel operations have undergone a rapid digital transformation over the past two decades, moving from paper-based registers to interconnected Property Management Systems (PMS), point-of-sale (POS) terminals, and cloud-based reservation platforms. This digitisation has delivered clear efficiency gains but has also progressively widened the attack surface available to threat actors, a pattern well documented across the global hospitality sector (Ravindu Denuwan Godag, 2018) and now increasingly visible in East African hotels such as LVH.

Theoretical Perspective

The study was steered jointly by Systems Theory (Pigola et al., 2025), Protection Motivation Theory (Maalem Lahcen et al., 2020), and Compliance and Regulatory Theory. Systems Theory frames the hotel's

cybersecurity posture as an interconnected whole in which a weakness in one subsystem (e.g., an unsegmented network) compromises the security of others. Protection Motivation Theory (PMT) explains staff and management security behaviour as a function of threat appraisal and coping appraisal, justifying the framework's emphasis on structured awareness training. Compliance and Regulatory Theory situate the framework within Uganda's DPPA 2019 and CMAA 2022 obligations, which create both a legal floor and a motivating pressure for control adoption.

Contextual Perspective

The study was undertaken at Lake Victoria Hotel, Entebbe, Uganda. This case was selected following a real ransomware attack in 2017, in which one user's computer was compromised via the internet, exposing the limits of the hotel's technical controls when its own systems became a point of failure. Technical assessments, supported by structured surveys, semi-structured interviews, and OpenVAS-assisted vulnerability scanning, confirmed critical control weaknesses: absent IDS/IPS and SIEM capabilities, no Next-Generation Firewall (NGFW), no Zero Trust Architecture enforcement, irregular patch management, no Incident Response Plan, and no documented access governance policy. These deficiencies are compounded by low staff cybersecurity awareness 64.3% of general staff reported having received no cybersecurity training and the confirmed use of shared, generic system accounts by all IT personnel, directly exposing guest PII and payment card data to unauthorised access, ransomware, and insider threats.

Conceptual Perspective

IT cybersecurity controls in this study are conceptualised across three categories administrative, technical, and physical that jointly determine the effectiveness of secure system and network access, itself operationalised through the CIA triad (confidentiality, integrity, availability), incident-rate reduction, and regulatory compliance. This conceptualisation underpins both the study's hypotheses and the structure of the resulting LVH-CCF.

Statement of the Problem

Hotels across the hospitality sector continue to invest in perimeter defences, antivirus, firewalls, and backups, yet critical preventive and governance controls, multi-factor authentication, documented security policy, network segmentation, and staff cybersecurity training, remain largely absent, leaving the underlying attack surface exposed. Lake Victoria Hotel experienced this directly in 2017, when a ransomware attack compromised a user's system via the internet despite existing technical defences. Regardless of the defences in place, cybersecurity training at LVH has continued to be delivered infrequently, generically, and without role differentiation, formal assessment, or governance accountability. Nearly two-thirds of staff (64.3%) had received no cybersecurity training at all, and all seven management respondents rated existing security measures as inadequate (M = 2.29 of 5) while unanimously endorsing a structured framework (M = 4.57). This has left interconnected systems, the PMS, POS, and CRM platforms, exposed through shared generic accounts, absent MFA, and unsegmented networks, directly threatening guest PII and payment card data. It is upon this basis that this study examined Lake Victoria Hotel's cybersecurity control gaps and designed a targeted framework, the LVH-CCF.

Objectives of the Study

Main Objective

To design and propose a robust cybersecurity controls framework for secure system and network access at Lake Victoria Hotel, Entebbe, Uganda, in alignment with NIST CSF 2.0, NIST SP 800-53 Rev. 5, and Uganda's regulatory requirements under the Data Protection and Privacy Act (DPPA) 2019 and the Computer Misuse (Amendment) Act (CMAA) 2022.

Specific Objectives

The study pursued three specific objectives:

1. To evaluate and propose access control measures, including Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), Privileged Access Management (PAM), and VLAN-based network segmentation, to secure LVH's systems and networks against unauthorised access.
2. To develop a comprehensive incident response and recovery plan, aligned to NIST SP 800-61 Rev. 3, to mitigate the impact of cyberattacks and ensure business continuity at Lake Victoria Hotel.
3. To design a cybersecurity controls framework for secure system and network access at Lake Victoria Hotel, anchored in internationally recognised standards and Uganda's legal obligations.

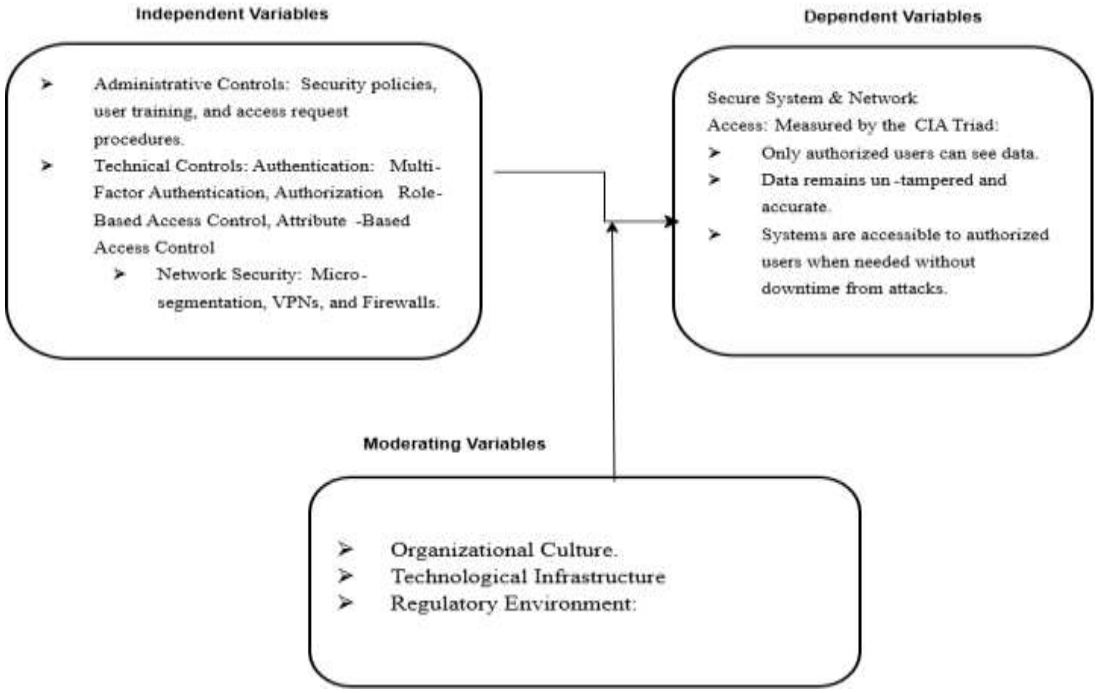
Study Hypothesis

H_1: Implementing the cybersecurity controls framework for secure system and network access at Lake Victoria Hotel, Entebbe, has a significant effect on the hotel's security posture.

H_2: Implementing the cybersecurity controls framework for secure system and network access at Lake Victoria Hotel, Entebbe, has no significant effect on the hotel's security posture.

Conceptual Framework

The Conceptual Framework displays the relationship between cybersecurity controls (Independent variables) and secure system and network access (dependent variables).



Literature Review

Cybersecurity Risk Exposure, Frameworks, and Regulatory Context in the Hospitality Sector

The hospitality industry's distinctive exposure to cyberattacks stems from the volume of sensitive guest data it processes, personally identifiable information (PII), payment card data, and loyalty records, combined with the operational pressure to sustain uninterrupted system availability. (Ravindu Denuwan Godag, 2018) documented the 2018 Marriott International breach, in which roughly 500 million guest records were exposed, illustrating the scale of risk that data-intensive hospitality operations carry.

(The NIST Cybersecurity Framework (CSF) 2.0, 2024) sets out NIST CSF 2.0 as a systematic, six-function structure, Govern, Identify, Protect, Detect, Respond, Recover, for managing cybersecurity risk across organisations of varying size and resource level, supplemented by NIST SP 800-53 Rev. 5's technical control catalogue. In Uganda, the DPPA 2019 and CMAA 2022 establish the legal boundaries within which hotel cybersecurity practices must operate, mandating technical and organisational security measures (Section 27), a lawful basis for processing (Section 5), and 72-hour breach notification (Section 29). This study's external expert respondents consistently identified the absence of sector-specific regulatory guidance as a gap limiting compliance uptake, a finding that directly informs the framework's regulatory-alignment component.

Individual studies converge on a consistent set of hospitality-specific vulnerabilities that this study's own findings confirm. (Wynn & Lam, 2023), (Pipyros & Liasidou, 2025), and (Shabani & Munir, 2020) collectively document flat network architectures, shared-credential use, reliance on basic antivirus as a primary endpoint defence, and staff awareness as the first line of defence against phishing as persistent weaknesses in hotel operations. On the mitigation side,(Bernardo et al., 2025) demonstrated that NIST CSF-aligned maturity assessment strengthens organisations' cybersecurity risk management, (Wynn & Lam, 2023) separately confirmed that multi-factor authentication, role-based access control, and network segmentation reduce unauthorised access in hotel environments, IBM's (2024) Cost of a Data Breach Report established that tested incident response plans reduce recovery time and cost, and (Shabani & Munir, 2020) showed that hotels' cyberattack-prevention techniques remain largely rudimentary.

A critical gap persists, however: the empirical literature is dominated by studies from developed economies and technology-intensive industries, while cybersecurity framework implementation in the hospitality sector in Sub-Saharan Africa, and Uganda specifically, remains almost entirely unexamined. No prior study integrates NIST CSF 2.0, NIST SP 800-53 Rev. 5, Uganda's DPPA 2019, and multi-stakeholder evidence from management, IT personnel, staff, external experts, and guests into a single, empirically validated cybersecurity controls framework for a Ugandan hospitality organisation. The present study addresses this gap directly.

Methodology

Research Design

The study adopted a Sequential Explanatory Mixed-Methods Design, qualitative-dominant (QUAL-quan), in which quantitative data collection in Phase 1 informed the qualitative phase in Phase 2 (Levitt et al., 2018), nested within a case study strategy (Ma et al., 2017) suited to examining a contemporary phenomenon within its real-world organisational context. In Phase 1, structured surveys measured staff cybersecurity awareness, risky behaviours, and perceptions of existing controls, analysed with descriptive and inferential statistics. In Phase 2, semi-structured interviews with management, IT personnel, and

external experts, together with OpenVAS-assisted technical audits, provided contextual explanation of the patterns identified and informed the framework's control specifications.

Study population and Sample Size

The study population comprised five segments: hotel management decision-makers; IT personnel responsible for systems and networks; general staff across operational departments; external cybersecurity and regulatory experts; and hotel guests. A target purposive sample of 150 was set at proposal stage; fieldwork constraints at an operational hospitality site yielded a realised sample of 72 respondents, summarised in Table 2.

Table 1: Respondent Distribution by Group

Department /Category	Population	Sample	%	Instrument
Hotel Management	20	7	9.7	Interview + Survey
IT Personnel	4	3	4.2	Interview + System Audit
General Staff	18	14	19.4	Structured Survey
External Experts	15	5	6.9	Semi-structured Interview
Hotel Guests	43	43	59.7	Structured Survey
Total	100	72	100.0	

Table 1: Respondent Distribution by Group (N = 72)

Data Collection and Analysis

Primary data were collected through structured surveys and semi-structured interviews administered across five stakeholder groups (management, IT personnel, general staff, external experts, and hotel guests), supplemented by OpenVAS-assisted vulnerability scanning of the hotel's IT infrastructure, yielding a realised sample of 72. Secondary data comprised existing internal documentation at Lake Victoria Hotel, including IT policies, incident reports, and previous audit findings, supplemented by Uganda's Data Protection and Privacy Act (2019), the Computer Misuse (Amendment) Act (2022), and industry threat intelligence reports on the hospitality sector's cybersecurity risk landscape. Data were analysed in IBM SPSS using descriptive statistics (frequencies and percentages), a Wilcoxon Signed-Rank test, a Spearman correlation, and a Chi-Square Test of Independence, at a significance level of $p < 0.05$.

Study Findings

Demographic Composition of Respondents

The study gauged the demographic characteristics of the 72 respondents. The results are in percentages in the table 2.

Category	Items	Frequency	Percentage (%)
Respondent Group (n = 72)	Hotel Guests	43	59.7
	General Staff	14	19.4
	Hotel Management	7	9.7

Category	Items	Frequency	Percentage (%)
	External Experts	5	6.9
	IT Personnel	3	4.2
	Total	**72**	**100.0**
Staff Department (n = 14)	Finance	5	35.7
	Front Desk	3	21.4
	Reservations	3	21.4
	Housekeeping	3	21.4
	Restaurant	0	0.0
Staff Education Level (n = 14)	A Level / Diploma	6	42.9
	Bachelor's Degree	5	35.7
	O Level Certificate	2	14.3
	Postgraduate	1	7.1
Staff Cybersecurity Training (n = 14)	No training received	9	64.3
	Trained in the past	3	21.4
	Recently trained	2	14.3
Guest Nationality (n = 43)	International Visitors	20	46.5
	Ugandan Nationals	12	27.9
	East African Visitors	9	20.9
	Other African Countries	2	4.7
Guest Visit Frequency (n = 43)	First-time Visitors	20	46.5
	Occasional Visitors	14	32.6
	Regular Guests	9	20.9

Table 2 shows that hotel guests formed the largest respondent group (59.7%, n = 43), followed by general staff (19.4%, n = 14), reflecting the study's dual focus on guest data-protection perceptions and staff cybersecurity practice. Among staff, 64.3% (n = 9) had received no cybersecurity training at all, revealing a significant awareness gap that directly informs the framework's staff-facing controls. Guests were similarly diverse, with international visitors forming the largest share (46.5%, n = 20) and an equal 46.5% being first-time visitors, indicating varied familiarity with the hotel's data-handling practices among the population the framework is designed to protect.

Relationship Between Multi Factor Authentication and Unauthorised Access

This validates an integrated approach to access control one that combines technical enforcement (MFA, RBAC) with behavioural reinforcement (structured awareness training) which is precisely the approach taken within the proposed framework.

It should be noted that this study did not collect direct outcome data on unauthorised-access incident rates at LVH; the relationship between MFA and unauthorised access is therefore established through convergent descriptive evidence and theoretical inference rather than inferential statistics. Both management and IT personnel independently confirmed that MFA is absent from every system at the hotel (0%), a fact reinforced by the low IT self-rating of access control effectiveness (M = 2.33). Systems Theory offers a mechanistic explanation for why this matters: LVH's tightly coupled PMS, POS, and network infrastructure means that a single unauthorised entry point can propagate to compromise the wider system. This is corroborated empirically by Wynn and Lam (2023), whose quantitative study of 120 IT professionals across European and Asian hotels found that MFA, together with RBAC and network segmentation, materially reduces unauthorised access in comparable hospitality environments. Taken together, LVH's complete absence of MFA places the hotel within the elevated-risk profile identified in that literature, even though this study did not directly measure the hotel's own unauthorised-access incident rate.

Experts Validations

External expert assessments (n = 5) converged on a clear design mandate for the LVH-CCF. Experts rated unauthorised system access as the most severe threat facing the hotel (M = 4.40), closely followed by weak/shared passwords and unpatched systems (both M = 4.20), directly justifying the framework's heaviest weighting toward the PROTECT function (16 of 39 controls, 41% of the total). Four control gaps were flagged as critical by 80% of experts the absence of MFA/RBAC, SIEM/IDS/IPS, a documented Incident Response Plan, and vulnerability scanning and each maps directly onto a Critical-priority control in the proposed framework (PR-01 MFA, PR-02 RBAC, DE-01 SIEM, RS-01 IRP, ID-03 vulnerability scanning). All five experts endorsed NIST CSF 2.0 as a suitable anchor standard provided it was localised to the Ugandan hospitality context, with PROTECT (M = 4.60) and IDENTIFY (M = 4.40) rated the most immediately applicable functions and GOVERN and RECOVER (both M = 3.60) flagged as needing the greatest local adaptation a distinction reflected in the framework's phased rollout, which sequences access-control hardening ahead of governance and recovery maturation. This expert evidence, triangulated against the IT personnel and management findings, provided the empirical justification for both the framework's control inventory and its priority tiering**.**

The Proposed IT Cybersecurity Controls Framework

The LVH-CCF comprises 39 controls distributed across the six NIST CSF 2.0 functions: Govern (6), Identify (5), Protect (16), Detect (4), Respond (4), and Recover (4). Of these, 20 are classified as Critical, 17 as High, and 2 as Moderate priority. The concentration of controls in the PROTECT function (16 controls, 41% of the total) reflects the empirical evidence that LVH's most urgent gaps lie in preventive technical controls MFA, RBAC, network segmentation, EDR, patch management, and awareness training each confirmed as absent or deficient by multiple respondent groups

Phase 1: Governance and Risk Foundation

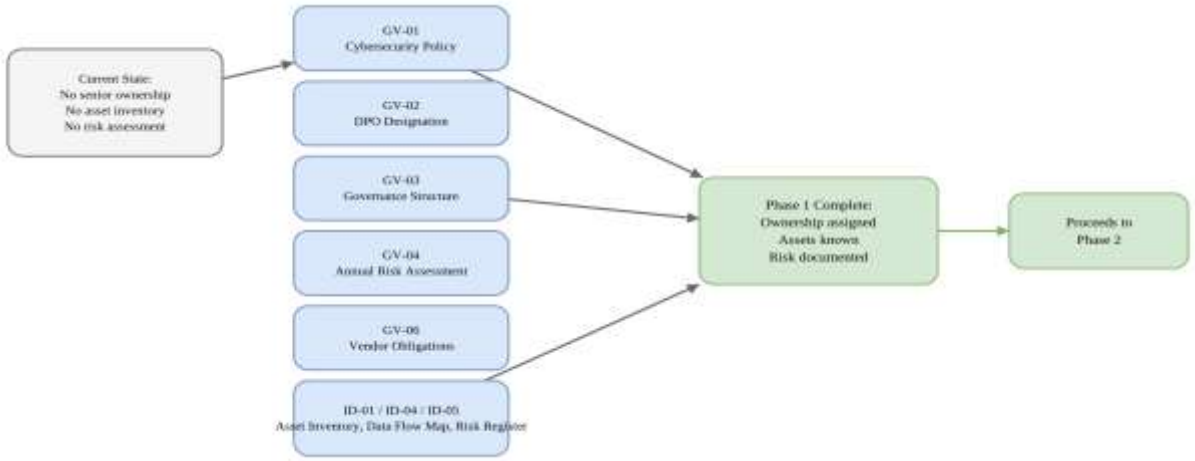


Figure 1: Phase 1, Governance and Risk Foundation. Source: Researcher's own design (2026).

Phase 1 lays the groundwork before any technical control goes in a formal cybersecurity policy, a designated Data Protection Officer, and an annual risk assessment cycle, backed by clear vendor security obligations. Alongside this, the hotel builds a full IT asset inventory and maps its data flows into a proper risk register. It comes first because you can't secure what you haven't inventoried, and you can't get buy-in without clear ownership and the evidence backs the priority: over 80% of experts flagged weak governance as the starting problem, which is exactly the gap this phase is built to close.

Phase 2: Access Control and Network Hardening

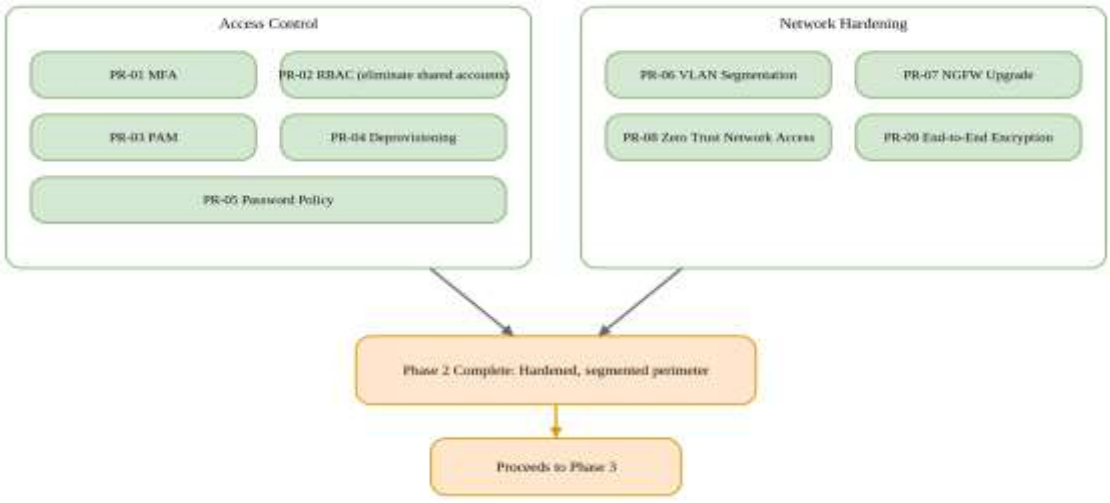


Figure 2: Phase 2, Access Control and Network Hardening. Source:

Phase 2 (Months 2–5) turns to access control the area where the hotel's IT setup was weakest, with every IT respondent flagging the same gaps: no MFA, shared generic logins, and a flat, unsegmented network. This phase introduces multi-factor authentication and role-based access control to retire those shared logins, tightens things further with least-privilege rules, privileged access management, and a proper password policy, and restructures the network with VLAN segmentation and an upgraded next-gen firewall. It follows governance because access control only means something once there's a policy and someone accountable behind it and it's arguably the most urgent phase, closing the hotel's most direct legal exposure under DPPA 2019 and addressing the single clearest, most unanimous finding across IT respondents.

Phase 3: Detection and Continuous Monitoring

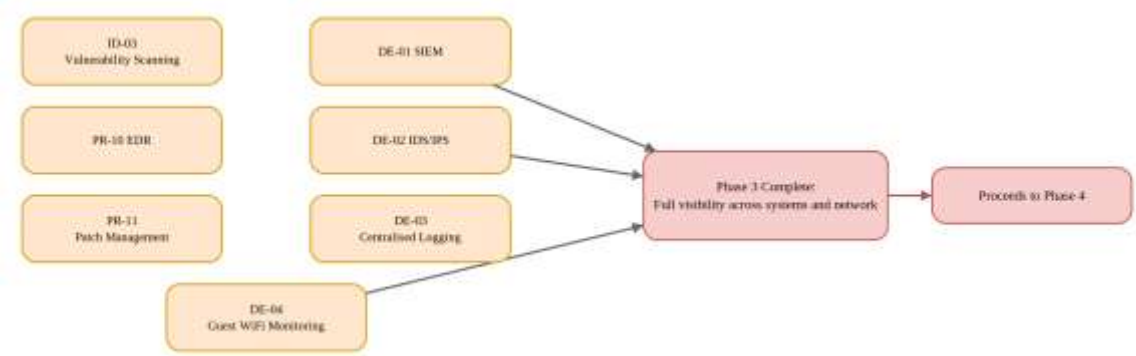


Figure 3: Phase 3, Detection and Continuous Monitoring. Source: Researcher's own design (2026).

Phase 3, shifts focus from access to visibility regular vulnerability scanning, patch management, and endpoint detection catch weaknesses early, while a SIEM system, intrusion detection, centralised logging, and guest WiFi monitoring give the hotel a consolidated view of what's happening across its network. It follows access control because monitoring only makes sense once the network is locked down, and it directly targets the survey's weakest-rated control area detection capability, which IT respondents scored lower than anything else measured.

Phase 4: Response, Recovery and Business Continuity

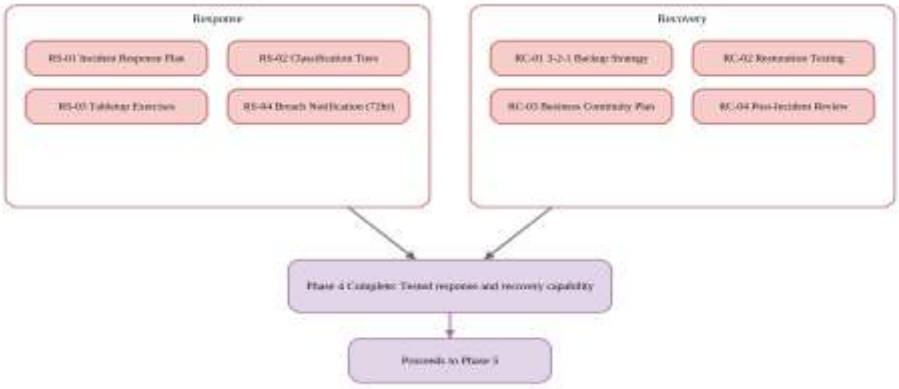


Figure 4: Phase 4, Response, Recovery and Business Continuity

By this stage, access is restricted and detection is in place, so the framework turns to what happens when something still gets through. This phase puts a documented incident response plan in place, with clear classification and escalation steps, tested through tabletop exercises, and a formal breach notification

procedure. On the recovery side, it introduces a 3-2-1 backup strategy with regular testing, manual fallback procedures to keep operations running during an outage, and a post-incident review process to capture lessons learned.

It comes fourth because response and recovery only work once there's something to detect the problem and a secure baseline to fall back on. And the evidence makes this phase hard to deprioritise: every single management respondent confirmed the same gap no documented plan, no tested backups making it the single most critical finding of the entire study.

Phase 5: Awareness, Data Governance and Continuous Improvement

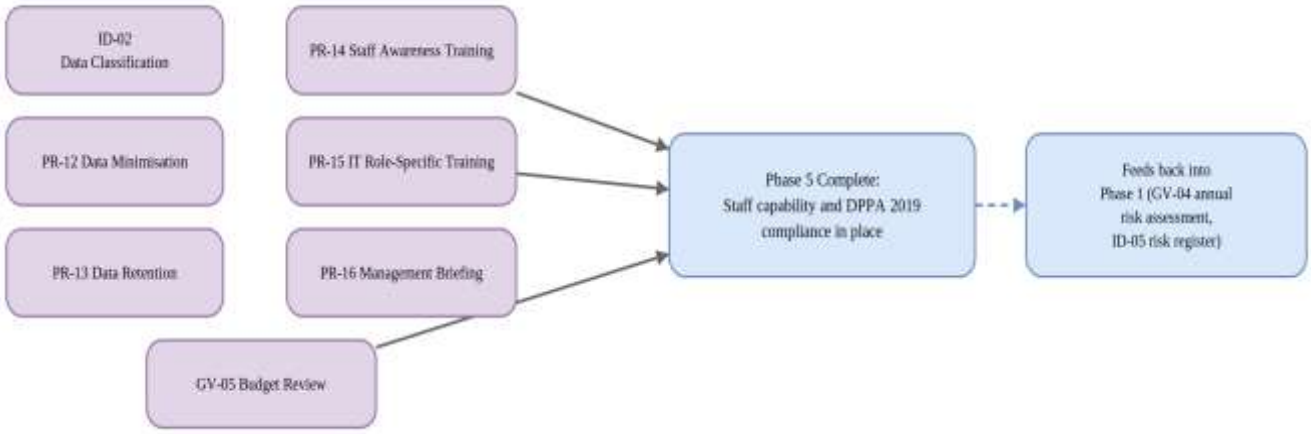


Figure 5: Phase 5, Awareness, Data Governance and Continuous Improvement.

By this point, the technical and procedural controls are in place, so the final phase turns to the people and processes that keep everything running. This means classifying data properly, applying data minimisation and retention rules, and rolling out awareness training across the board general staff training, IT-specific training, and a dedicated management briefing alongside a formal review of the cybersecurity budget to keep resourcing sustainable.

It comes last because it consolidates everything built in the earlier phases rather than introducing something new, and it directly answers the training gap flagged in the study, where roughly two-thirds of staff reported no cybersecurity training at all. Completing this phase brings the hotel to full data protection compliance and closes the loop: rather than ending, it feeds back into Phase 1, triggering the next annual risk assessment and an updated risk register, turning the framework into a recurring cycle instead of a one-time rollout.

Framework KPI Dashboard Baselines

The LVH-CCF was benchmarked against NIST CSF 2.0 (NIST, 2024), ISO/IEC 27001 (ISO/IEC, 2022), and generic hospitality compliance checklists, none of which combine phased, budget-sensitive control sequencing with dual DPPA 2019/CMAA 2022 alignment and severity-weighted success criteria drawn directly from the hotel's own respondent data, a combination the LVH-CCF provides and which the five external experts rated suitable for adoption, localisation required, without prior exposure to its design.

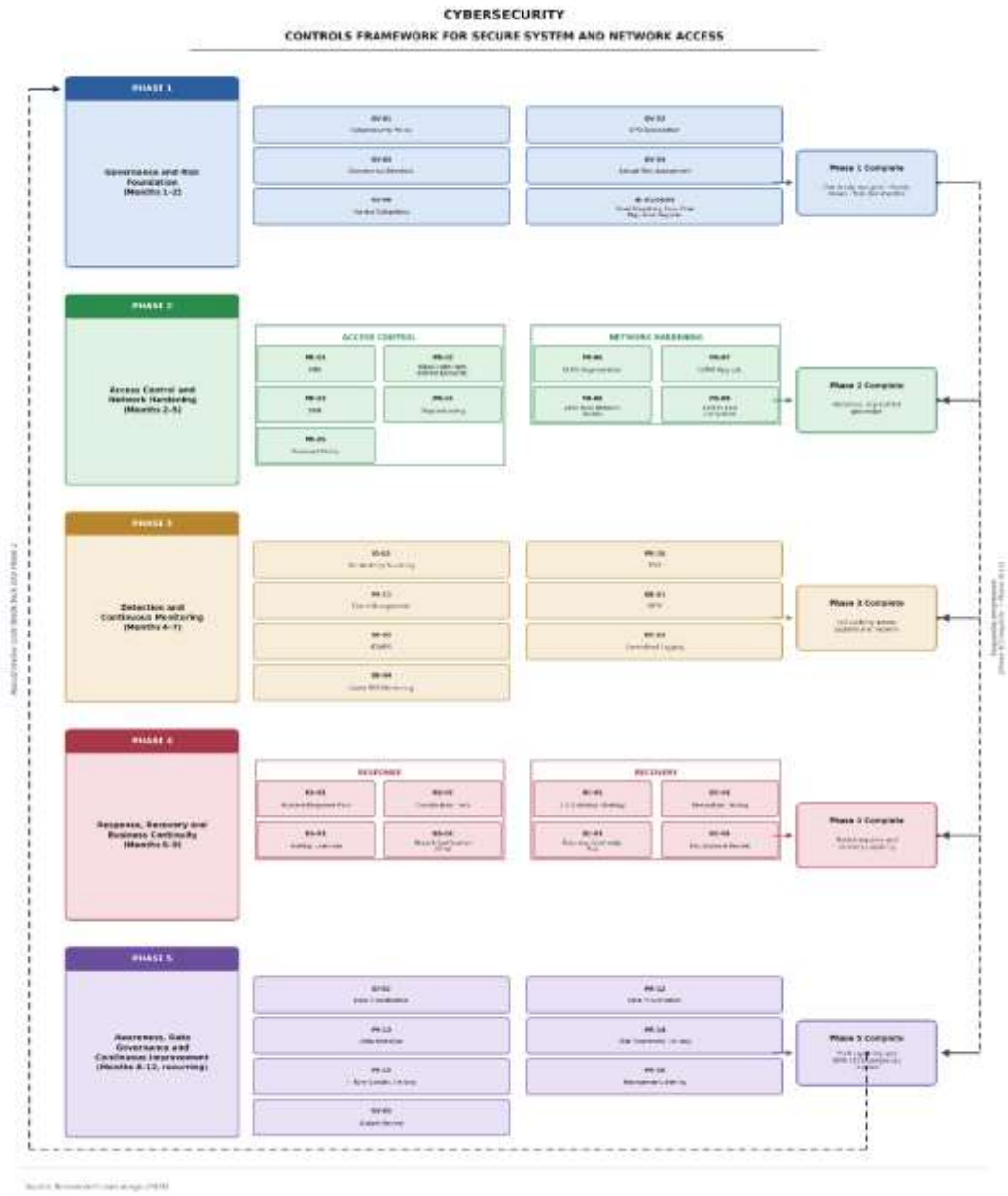


Figure 6 shows the full LVH-CCF roadmap, mapping all 39 controls to their governing NIST CSF 2.0 function across five phases, from governance foundations to the recurring awareness and improvement cycle feeding back into Phase 1.

Conclusion

The study concludes that the LVH-CCF is statistically and significantly associated with improved secure system and network access at Lake Victoria Hotel, evidenced by a significant Wilcoxon Signed-Rank result ($W = 5.000$, $p = 0.0196$) and a very strong correlation between password hygiene and threat recognition (Spearman $\rho = 0.922$, $p < 0.001$). The hotel's existing posture was structurally inadequate: shared generic accounts, absent MFA and privileged access management, minimal network segmentation, and no tested incident response plan. The incident-response link fell short of conventional significance ($\chi^2 = 6.222$, $p = 0.183$) but is reinforced by consistent qualitative evidence, including 80% of external experts

flagging IRP absence as critical. H_1 and H_2 are therefore supported; H_3 is supported qualitatively rather than statistically.

10. Recommendations

For Lake Victoria Hotel management: eliminate every shared, generic system account in favour of individually assigned, least-privilege accounts the single highest-impact, lowest-cost change available, confirmed as a universal gap by all IT respondents. Approve and resource the phased LVH-CCF roadmap, beginning with governance and risk foundations before committing to costlier detection and monitoring investments.

For the IT department: implement MFA and RBAC across all systems, deploy VLAN-based network segmentation separating the PMS, POS, and administrative systems, and introduce SIEM/IDS/IPS and EDR capability to close the study's most severe detection gap. Document and table-top test an Incident Response Plan aligned to the NIST SP 800-61 lifecycle and adopt a 3-2-1 backup strategy with regular restoration testing.

For human resources and staff training: institute a mandatory, quarterly, role-differentiated cybersecurity awareness programme grounded in Protection Motivation Theory, directly responding to the 64.3% of staff who currently report no training, and integrate cybersecurity performance into staff appraisal to reinforce accountability.

For policymakers and regulators: develop sector-specific technical guidance operationalising DPPA 2019 obligations for hospitality operators, closing the gap external experts identified between the law's general provisions and its practical application in resource-constrained hotel environments.

For future researchers: extend this study to a multi-hotel or national sample to test the transferability of the LVH-CCF, and evaluate framework effectiveness longitudinally following implementation to validate the projected reduction in incident rates and improvement in DPPA 2019 compliance.

References

1. Bernardo, L., Malta, S., & Magalhães, J. (2025). An evaluation framework for cybersecurity maturity aligned with the NIST CSF. Electronics, 14(7), Article 1364. https://doi.org/10.3390/electronics14071364
2. Chen, H. S., & Fiscus, J. (2018). The inhospitable vulnerability: A need for cybersecurity risk assessment in the hospitality industry. Journal of Hospitality and Tourism Technology, 9(2), 223–234. https://doi.org/10.1108/JHTT-07-2017-0044
3. IBM. (2024). Cost of a data breach report 2024. IBM Security. https://www.ibm.com/reports/data-breach
4. Joint Task Force. (2020). Security and privacy controls for information systems and organizations (NIST SP 800-53, Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5
5. Levitt, H. M., Bamberg, M., Creswell, J. W., Frost, D. M., Josselson, R., & Suárez-Orozco, C. (2018). Journal article reporting standards for qualitative primary, qualitative meta-analytic, and mixed methods research in psychology. American Psychologist, 73(1), 26–46. https://doi.org/10.1037/amp0000151
6. Muhangi, K. (2019). Overview of data protection regime in Uganda.

7. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
8. Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST SP 800-61, Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3
9. Perlroth, N., Tsang, A., & Satariano, A. (2018, November 30). Marriott hacking exposes data of up to 500 million guests. The New York Times.
10. Pipyros, K., & Liasidou, S. (2025). A new cybersecurity risk assessment framework for the hospitality industry: Techniques and methods for enhanced data protection and threat mitigation. Worldwide Hospitality and Tourism Themes, 17(1), 48–61. https://doi.org/10.1108/WHATT-12-2024-0296
11. Republic of Uganda. (2019). Data Protection and Privacy Act, 2019.
12. Republic of Uganda. (2022). Computer Misuse (Amendment) Act, 2022.
13. Shabani, N., & Munir, A. (2020). A review of cyber security issues in hospitality industry. In K. Arai, S. Kapoor, & R. Bhatia (Eds.), Intelligent computing: Proceedings of the 2020 Computing Conference (Vol. 1230, pp. 482–493). Springer. https://doi.org/10.1007/978-3-030-52243-8_35
14. Wynn, M., & Lam, C. (2023). Digitalisation and IT strategy in the hospitality industry. Systems, 11(10), Article 501. https://doi.org/10.3390/systems11100501
15. Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.