Hybrid Cybersecurity Compliance Audit Framework for an On-Premise Hotel Property Management System: Mapping NIST CSF 2.0 Controls to Indonesia's Personal Data Protection Law

I Made Sudana*
Master of Informatics
Universitas Muhammadiyah Surakarta
Surakarta, Indonesia
l208250008@student.ums.ac.id

Bana Handaga
Master of Informatics
Universitas Muhammadiyah Surakarta
Surakarta, Indonesia
bana@ums.ac.id

Jan Wantoro
Master of Informatics
Universitas Muhammadiyah Surakarta
Surakarta, Indonesia
jan@ums.ac.id

Abstract

The accelerating digitalization of Property Management Systems (PMS) in the hospitality sector introduces substantial cybersecurity exposure, particularly concerning the protection of guests' personal data. This study audits the cybersecurity posture of an on-premises e-VHP PMS operated by an international chain hotel in Surakarta, Indonesia, whose local PMS core is integrated with cloud-based third-party Channel Manager and Online Travel Agency (OTA) platforms managed at the corporate level. A hybrid audit instrument was developed to bridge technical controls under the NIST Cybersecurity Framework (CSF) 2.0 with legal obligations under Indonesia's Personal Data Protection Law (UU PDP) No. 27/2022. Primary data were collected through structured interviews with six informants representing three organizational layers: managerial (General Manager), technical (two IT Officers), and operational/front-line staff (Front Office, General Cashier/Accounts Payable, and Income Audit/Accounts Receivable), using a five-point maturity rubric (1 = Not Implemented to 5 = Optimized and Continuously Reviewed). Aggregated maturity scores showed that Detect (3.33) and Govern (3.00) achieved the highest relative maturity, whereas Respond (1.50) and Recover (1.89) showed the most severe capability deficits; Protect (2.50) and Identify (2.44) fell in between. Gap analysis against the optimal target (5.00) placed Respond at the highest remediation priority (Gap = 3.50), followed by Recover (Gap = 3.11). A structured risk register identified critical exposure in endpoint backup failure and unmanaged credential sharing among front-line staff, alongside high power-management and integration-channel risks. Structural mapping shows these technical and behavioral gaps correspond to potential non-compliance with Articles 35, 39, and 46 of the UU PDP, exposing the organization to administrative fines of up to 2% of annual revenue. The study proposes a tiered Cybersecurity Governance Blueprint emphasizing local incident-response

* Corresponding Author

capability, standardized power-backup procurement, encrypted endpoint backup automation, and a structured security-awareness program for front-line personnel.

Keywords: cybersecurity audit, hotel PMS, NIST CSF 2.0, Personal Data Protection Law (UU PDP), multi-stakeholder risk assessment

Introduction

The rapid digitalization of hotel operations through Property Management Systems (PMS) has expanded the cyber-attack surface of the hospitality industry, which manages highly sensitive guest data, including Personally Identifiable Information (PII), passport records, and payment credentials (Karadayi-Usta, 2024; Pipyros & Liasidou, 2025). In Indonesia, this exposure is compounded by the enactment of Law No. 27 of 2022 on Personal Data Protection (UU PDP), which imposes substantial administrative and criminal liability on data controllers that fail to safeguard consumer data (Sari et al., 2023; Wibowo et al., 2023).

Within hotel operations, security responsibility is frequently distributed across a Shared Responsibility Model that is more fragmented than the conventional cloud-vendor/customer dichotomy typically discussed in the literature. Field evidence collected for this study indicates that the audited property's PMS core operates on-premises, within a closed local network, while cloud-based connectivity is confined to a centrally managed Channel Manager integration linking the property to third-party Online Travel Agencies (OTAs). This hybrid on-premise/cloud-integration architecture means that local management retains direct operational responsibility for physical infrastructure resilience (power continuity, endpoint backup, local access control), while encryption and integration-channel security for external data flows are governed at the corporate level. This nuance is rarely addressed in prior literature, which tends to assume either a fully cloud-hosted PMS or a fully isolated on-premises system (Demir & Demir, 2025; Kim et al., 2013).

Prior research has generally bifurcated into two strands: technical cybersecurity maturity assessments that do not engage legal compliance implications (Bernardo et al., 2025; Casaril & Galletta, 2025), and legal-compliance studies that address regulatory obligations without operational or infrastructural specificity (Voigt & Von dem Bussche, 2017). Few studies integrate multi-stakeholder field evidence spanning managerial, technical, and front-line operational perspectives into a single audit instrument that links infrastructural weaknesses to specific statutory provisions.

This study addresses that gap by implementing a hybrid audit instrument that integrates: (1) standardized technical controls based on NIST CSF 2.0, (2) a structured risk quantification approach informed by triangulated interview data from six respondents across three organizational layers, and (3) structural mapping of audit findings to specific UU PDP provisions. The resulting Cybersecurity Governance Blueprint is intended to support continuous, evidence-based compliance rather than a one-time, point-in-time assessment.

To address this gap, this study proposes a novel Hybrid Cybersecurity Compliance Framework that systematically integrates the technical sub-categories of the NIST Cybersecurity Framework (NIST CSF 2.0), specifically the *Protect* and *Detect* functions, with the statutory data governance mandates of the UU PDP Law. Unlike conventional case-based audits that merely report post-hoc compliance failures, the theoretical contribution of this research lies in establishing a structured, risk-prioritized mapping mechanism. This framework provides a replicable conceptual bridge that translates technical host and network hardening metrics directly into legal compliance maturity levels for hospitality operations.

- A traceable audit artifact systematically mapping NIST CSF 2.0 sub-categories to specific UU PDP statutory obligations addressing a methodological gap in the Indonesian regulatory landscape.
- The first multi-layer empirical evidence detailing the security posture of hybrid on-premise/cloud-integrated hotel PMS architectures.

- A conceptual bridge demonstrating how physical infrastructure gaps (e.g., power continuity, local backup failures) map directly to statutory legal exposures under data protection laws.

Literature Review

Research on information-system audits and cybersecurity governance across industries commonly adopts international standard frameworks such as the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001 as primary references for evaluating information-technology security posture (Culot et al., 2021). Much of this literature concentrates on banking and critical-network environments, given their high material-loss exposure (Abbas & Alazawi, 2026), and demonstrates that NIST CSF and ISO/IEC 27001 are effective for mapping security gaps, identifying network-penetration threats, and periodically measuring cyber-capability maturity (Abbas & Alazawi, 2026; Bernardo et al., 2025; Brezavšček & Baggia, 2025). However, these studies typically evaluate rigid information-system architectures supported by dedicated internal IT teams (Büyüközkan & Güler, 2025), so their resulting recommendations are often difficult to apply directly to organizations with more dynamic operations and limited on-site IT staffing.

A second strand of literature addresses the legal dimension of data security and privacy regulation, both global instruments such as the General Data Protection Regulation (GDPR) in Europe and domestic instruments such as Indonesia's UU PDP, which has grown substantially in recent years (Republik Indonesia, 2022; Voigt & Von dem Bussche, 2017). This strand generally focuses on organizational compliance readiness from a legal, data-governance, and macro risk-management perspective (Badawi et al., 2026), examining how UU PDP provisions shape data-controller obligations and legal certainty (Sari et al., 2023; Wibowo et al., 2023). While this work contributes significantly to the legal dimension, it generally lacks applicable operational or technical guidance, remaining largely theoretical-juridical and offering little direct intervention for site-level hardware or infrastructural failures. These studies have not yet bridged how physical anomalies, such as the absence of backup power at a core router or failure of endpoint backup systems, can directly satisfy the elements of a data-protection-regulation violation.

Given the limitations of both research strands, studies specifically auditing cybersecurity within hotel Property Management Systems (PMS) remain underdeveloped. Most conventional hospitality-technology research evaluates information-technology adoption from the standpoint of investment strategy, operational efficiency, or macro-level technology utilization (Demir & Demir, 2025; Cobanoglu et al., 2021), often overlooking the fact that integrating hotel information systems with third-party platforms creates an attack surface highly susceptible to data-security incidents (Karadayi-Usta, 2024; Kim et al., 2013). Where hospitality-sector cybersecurity research does exist, its scope is typically limited to generic risk-assessment techniques or macro-level threat awareness rather than in-depth audits of the underlying local infrastructure (Campoverde-Molina & Luján-Mora, 2025; Pipyros & Liasidou, 2025). Consequently, the hospitality industry may develop a false sense of security from adopting internationally branded information systems while remaining unaware of latent vulnerabilities in local infrastructure.

This study addresses this research gap by integrating the technical defenses of NIST CSF 2.0 with the legal-compliance obligations of UU PDP No. 27/2022 through a hybrid, multi-stakeholder audit approach (National Institute of Standards and Technology, 2024; Republik Indonesia, 2022). In contrast to prior single-method, single-informant studies, this research translates field-level infrastructural findings such as inconsistent UPS coverage and unrealized endpoint backup routines into concrete legal-compliance risk implications, triangulated across managerial, technical, and front-line respondents. Rather than assuming a one-time, absolute compliance state, this study adopts a feedback-loop perspective that treats legal-compliance assurance as a continuous, adaptive governance process (Badawi et al., 2026).

Theoretical Framework

To move beyond a descriptive audit report and establish robust explanatory power, this study anchors its analysis on two foundational theories: Socio-Technical Systems (STS) theory and Institutional Theory (Coercive Isomorphism).

- Socio-Technical Systems (STS) Theory: Originating from Trist and Bamford, STS posits that organizational performance depends on the optimization of both technical subsystems (hardware, software, networks) and social subsystems (people, policies, behaviors). In the context of a hybrid hotel PMS, technical security controls alone are insufficient if the social subsystem, such as front-line staff sharing passwords or handling unverified credentials, fails. This theory justifies our multi-layer assessment approach (managerial, technical, and operational).
- Institutional Theory (Coercive Isomorphism): Drawing on DiMaggio and Powell, coercive isomorphism explains how formal external pressures such as Indonesia's Personal Data Protection Law (UU PDP No. 27 of 2022) force organizations to adopt structural changes. However, organizations often exhibit *decoupling*, wherein formal corporate policies (*Govern* functions) are ceremonially adopted, while operational implementation and incident response capabilities (*Respond* and *Recover* functions) lag behind due to a lack of local technical capacity.

From these theories, two core propositions are formulated and examined through our empirical data:

- P_1 In organizations with centralized corporate IT, maturity scores for high-level governance (*Govern*) and detection (*Detect*) will be significantly higher than local execution capabilities (*Respond* and *Recover*), reflecting weak coupling across socio-technical subsystems.
- P_2 Regulatory pressures primarily induce documentary compliance rather than operational behavioral shifts, leading to structural decoupling between policy mandates and front-line practices.

Table 1. Summary of Related Literature and Positioning of This Study

Study	Sector	Framework / Standard	Informants / Layers	Legal Mapping	Instrument Validation	System Architecture
Bernardo et al. (2025)	General	NIST CSF	–	No	–	–
Pipyros & Liasidou (2025)	Hospitality	Risk Assessment	–	No	–	–
Karadayi-Usta (2024)	Hospitality	Stakeholder Model	–	No	–	–
Voigt & Von dem Bussche (2017)	Cross-sector	GDPR	–	Yes (legal only)	–	–
This Study	**Hospitality (PMS)**	**NIST CSF 2.0 × UU PDP**	**6 respondents, 3 layers**	**Yes, traceable per article**	**Yes (CVI + ICC)**	**Hybrid on-premise / cloud-integrated**

Table 1 presents a comparison of previous studies based on sector, framework or standard, informants and organizational layers, legal mapping, instrument validation, and system architecture. The comparison indicates that previous studies have addressed cybersecurity and data protection from different perspectives, but these dimensions have generally been examined separately.

Bernardo et al. (2025) applied the NIST Cybersecurity Framework (NIST CSF) to address cybersecurity assessment in a general context. Although the study provides a relevant cybersecurity framework, it does not specifically address the hospitality sector, legal mapping to data protection regulations, or the characteristics of hotel information system architecture. Pipyros & Liasidou (2025) focused on cybersecurity risk assessment within the hospitality sector, demonstrating the importance of risk-based approaches in hotel environments. However, the study does not explicitly integrate cybersecurity controls with applicable data protection legislation or provide a validated assessment instrument. Similarly, Karadayi-Usta (2024) emphasized stakeholder perspectives in the hospitality context, but did not combine stakeholder assessment with a formal cybersecurity framework, legal requirements, and technical system architecture.

Voigt & Von dem Bussche (2017), in contrast, provide a legal perspective through the General Data Protection Regulation (GDPR). Their work is important for understanding data protection obligations; however, the legal perspective is not directly integrated with a technical cybersecurity control framework, multi-layer organizational assessment, or empirical validation of an assessment instrument. Thus, while these studies provide valuable foundations, the comparison reveals that cybersecurity frameworks, hospitality risk assessment, stakeholder perspectives, and legal compliance have largely been addressed as separate components rather than as an integrated assessment approach.

The gap becomes particularly relevant in modern hotel Property Management Systems (PMS), where information processing occurs across organizational and technological boundaries. A hotel PMS may operate through on-premises infrastructure while simultaneously connecting to cloud-based Channel Managers and multiple Online Travel Agencies (OTAs). Consequently, cybersecurity governance cannot be evaluated solely from the perspective of internal technical controls or organizational policies. It also requires consideration of data protection obligations, stakeholder responsibilities, operational practices, and the shared responsibility between on-premises and cloud-based environments.

In response to this gap, the present study proposes an integrated assessment approach that combines NIST CSF 2.0 and Indonesia's Personal Data Protection Law (UU PDP) within the context of a hotel PMS. The study further incorporates six respondents across three organizational layers managerial, technical, and operational/front-line to support multi-perspective assessment and data triangulation. In addition, the assessment instrument is validated using the Content Validity Index (CVI) and Intraclass Correlation Coefficient (ICC), strengthening the methodological reliability of the proposed assessment.

Another distinguishing feature of this study is its explicit consideration of a hybrid on-premise/cloud-integrated system architecture. This allows the assessment to account for cybersecurity risks and responsibilities associated not only with the hotel's internal PMS infrastructure but also with external cloud-based integrations and OTA connectivity. Furthermore, the legal mapping is designed to be traceable to relevant provisions of the UU PDP, enabling cybersecurity controls to be evaluated alongside their corresponding legal obligations.

Therefore, compared with the previous studies presented in Table 1, this study contributes an integrated approach that connects cybersecurity controls, legal compliance, organizational perspectives, validated assessment instruments, and hybrid system architecture. The assessment results are subsequently translated into risk prioritization and a Hybrid Cybersecurity Governance Blueprint, providing a structured pathway from system diagnosis and control assessment to practical cybersecurity governance recommendations for hotel PMS environments.

Methodology

Research Design and Site

This study used a descriptive quantitative audit design combined with qualitative triangulation (mixed-methods) and was conducted at an international chain hotel property located in Surakarta, Central Java, Indonesia (hereafter referred to as "Hotel X" to preserve organizational confidentiality, consistent with the consent terms granted by site management). Data collection took place in June 2026. Hotel X operates an on-premise e-VHP PMS integrated, via a centrally managed Channel Manager, with cloud-based OTA distribution channels. Before data collection, the audit protocol, including the interview

instrument and the confidentiality terms governing the disclosure of site-level findings, was reviewed and approved by site management, and verbal informed consent was obtained from each respondent.

This study adopts a systematic, multi-phase evaluation methodology structured into four sequential phases to bridge technical cybersecurity metrics with regulatory compliance obligations within a hybrid hotel Property Management System (PMS) environment. The overall research flow, illustrated in Figure 1, is designed to ensure methodological rigor, moving from diagnostic scoping to framework formulation.

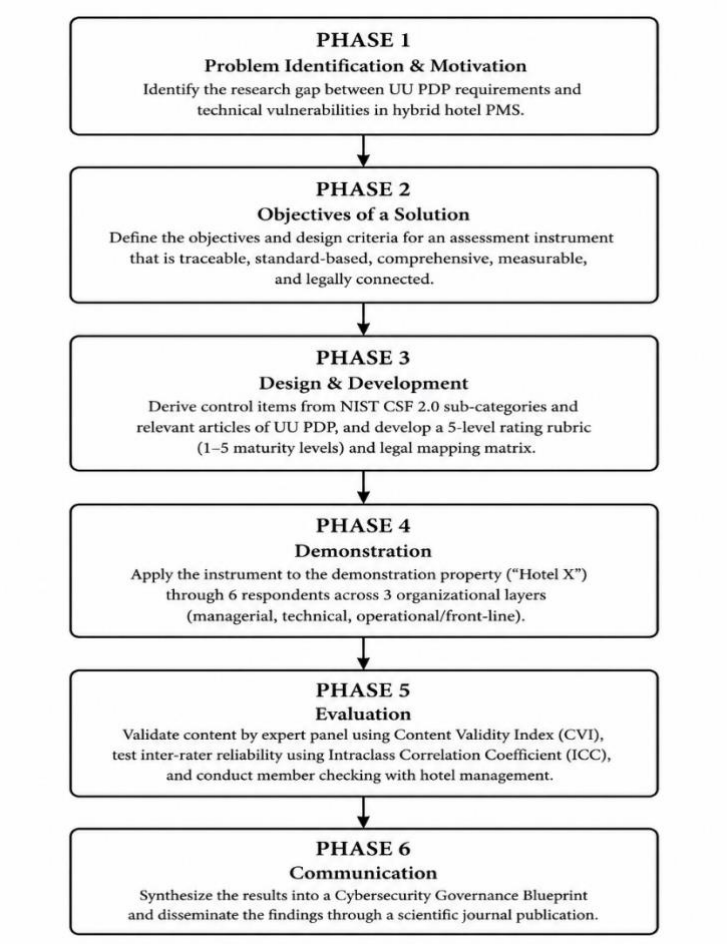


Figure 1. Six-Phase Research Methodological Flow for the Development and Evaluation of a Hybrid Hotel PMS Cybersecurity Governance Assessment

Phase 1: Problem Identification and Motivation

The first phase establishes the research problem and its underlying motivation. The study begins by identifying the gap between the requirements of Indonesia's Personal Data Protection Law (UU PDP) and the technical and organizational cybersecurity conditions of a hybrid hotel PMS environment. The problem is particularly relevant because contemporary hotel PMS environments increasingly operate across interconnected infrastructures, including on-premise servers and databases, cloud-based services, Channel Managers, and Online Travel Agencies (OTAs). Such interconnectedness creates multiple points at which personal and operational data may be processed, transmitted, stored, or accessed.

At this stage, the study examines the cybersecurity and data protection context of the hotel PMS and identifies potential discrepancies between regulatory expectations and actual technical or organizational practices. The analysis provides the basis for defining the research problem, establishing the research scope, and formulating the research gap. The output of this phase is therefore a clearly defined problem

statement and research motivation that justify the need for a context-specific cybersecurity assessment approach.

Phase 2: Objectives of a Solution

Following the identification of the problem, Phase 2 defines the objectives and design requirements of the proposed solution. The primary objective is to develop an assessment instrument capable of evaluating cybersecurity controls within a hybrid hotel PMS environment while maintaining clear relationships between technical controls, recognized cybersecurity standards, and applicable legal requirements.

Several design criteria are established in this phase. The instrument must be traceable, standard-based, comprehensive, measurable, and legally connected. Traceability requires that assessment items can be linked to their underlying cybersecurity control and corresponding legal provisions. The standard-based requirement is addressed through the use of the NIST Cybersecurity Framework (CSF) 2.0, while the legal dimension is incorporated through the mapping of relevant provisions of the UU PDP. The instrument must also be sufficiently comprehensive to address relevant cybersecurity practices, measurable through a consistent maturity-rating mechanism, and applicable to the organizational and technical characteristics of a hybrid hotel PMS. The output of this phase is a set of explicit instrument-design objectives and a conceptual framework that determines how NIST CSF 2.0 and UU PDP requirements will subsequently be integrated.

Phase 3: Design and Development

Phase 3 translates the objectives established in Phase 2 into the actual assessment instrument. In this stage, relevant control dimensions are derived from the selected NIST CSF 2.0 sub-categories, particularly those associated with the Protect and Detect functions. These control dimensions are then mapped to relevant provisions of the UU PDP to establish a legally traceable relationship between cybersecurity practices and personal data protection obligations.

The design process involves the development of assessment items, indicators, and a structured legal mapping matrix. Each assessment item is formulated to represent an observable cybersecurity practice or control that can subsequently be assessed within the hotel PMS environment. The mapping process is designed to preserve traceability, allowing each relevant control or assessment item to be associated with the corresponding legal provision.

A five-level maturity-rating rubric is also developed to support consistent assessment. The maturity scale ranges from Level 1 (Initial) to Level 5 (Optimized), representing progressive levels of cybersecurity capability and control maturity. The resulting draft instrument therefore consists of assessment items, control indicators, legal mappings, and a standardized rating mechanism. This phase produces the initial methodological artifact that will be applied and subsequently evaluated.

Phase 4: Demonstration

Phase 4 demonstrates the practical application of the developed instrument within an actual hotel PMS environment, represented in the study as “Hotel X.” The demonstration provides an empirical context in which the proposed assessment approach can be applied to a hybrid PMS architecture and its associated organizational processes. Data are collected from six respondents representing three organizational layers, namely the managerial layer, technical layer, and operational/front-line layer. The managerial layer provides evidence concerning governance, policies, and organizational oversight. The technical layer provides evidence concerning system configurations, technical controls, logs, backups, and infrastructure-related practices. The operational/front-line layer provides evidence concerning the actual day-to-day use of the PMS and operational security practices.

The use of multiple organizational layers enables the study to capture different dimensions of cybersecurity practice rather than relying on a single source of evidence. Data obtained through interviews, questionnaires, documentary evidence, technical walkthroughs, and relevant observations are subsequently compared and triangulated. This process enables the study to identify similarities,

inconsistencies, and gaps between documented policies, technical implementation, and operational practices.

The output of the demonstration phase is the empirical dataset and preliminary assessment results obtained from the application of the proposed instrument in the hotel PMS environment.

Phase 5: Evaluation

Phase 5 focuses on establishing the validity, reliability, and contextual credibility of the developed instrument and the resulting assessment. The evaluation consists of three complementary components: content validation, inter-rater reliability assessment, and member checking.

- First, the content of the instrument is evaluated by an expert panel using the Content Validity Index (CVI). This process determines whether the assessment items adequately represent the intended cybersecurity and data protection constructs and whether the items are relevant to the research objectives.
- Second, the consistency of assessments among raters is examined using the Intraclass Correlation Coefficient (ICC). The ICC provides an empirical basis for evaluating inter-rater reliability and determining whether the assessment produces sufficiently consistent ratings when applied by different evaluators.
- Third, member checking is conducted with hotel management to confirm the interpretation of findings and ensure that the assessment results appropriately reflect the actual organizational and operational context. Feedback obtained through this process is used to clarify or revise relevant elements where necessary. The combination of CVI, ICC, and member checking strengthens the methodological rigor of the study by addressing different dimensions of quality: content validity, measurement reliability, and contextual credibility. The output of this phase is a validated and reliable assessment instrument together with refined assessment findings.

Phase 6: Communication

The final phase translates the research findings into practical and scholarly outputs. The validated assessment results are analyzed to identify cybersecurity weaknesses, maturity gaps, and priority risks within the hybrid hotel PMS environment. These findings are then synthesized into a Cybersecurity Governance Blueprint that provides a structured basis for improving cybersecurity governance.

The blueprint is intended to connect assessment findings with practical governance responses, including cybersecurity priorities, control recommendations, governance mechanisms, and potential implementation directions. In this way, the research does not terminate at the identification of cybersecurity deficiencies but translates empirical findings into an actionable governance-oriented output.

At the scholarly level, the findings, methodological approach, instrument development, validation results, and governance implications are consolidated into the present scientific manuscript. Thus, communication serves two purposes: disseminating the research contribution to the academic community and providing a practical governance reference for organizations managing hybrid hotel PMS environments.

Instrument and Respondents

The audit instrument consisted of structured interview checklists derived from NIST CSF 2.0 functions (Govern, Identify, Protect, Detect, Respond, Recover), supplemented by two targeted sub-instruments: a Human-Factor checklist (front-line security awareness) and an Access-Control checklist (least-privilege and credential-handling practices). Each item was scored using a five-point maturity rubric, summarized in Table 2.

Table 2. Five-point Maturity Rubric Applied in the Field Instrument

Score	Maturity Level	Description
1	Not Implemented	Control is absent.
2	Inconsistent	Control exists but is applied irregularly or is undocumented.
3	Implemented	Control is applied as a standard practice.
4	Implemented & Monitored	Control is applied and actively monitored.
5	Optimized & Reviewed	Control is optimized and periodically evaluated.

Data were collected through structured interviews with six respondents purposively selected to represent three organizational layers directly responsible for, or affected by, cybersecurity controls: (1) managerial the General Manager; (2) technical two IT Officers; and (3) operational/front-line a Front Office Leader, a General Cashier/Accounts Payable officer, and an Income Audit/Accounts Receivable officer (Table 3). This multi-layer sampling strategy was adopted to triangulate self-reported managerial policy claims against technical implementation evidence and front-line behavioral reality, addressing a key methodological limitation: reliance on single-informant data identified in prior single-respondent audit studies.

Table 3. Respondent Profile

Respondent	Role	Instrument Scope
R1	IT Officer	Govern, Identify, Protect, Detect, Respond, Recover
R2	IT Officer	Govern, Identify, Protect, Detect, Respond, Recover
R3	General Manager	Govern, Identify, Protect, Detect, Respond, Recover
R4	Front Office Leader	Human Factor (security awareness)
R5	General Cashier / Accounts Payable	Access Control
R6	Income Audit / Accounts Receivable	Access Control

For items assessed by the three managerial/technical respondents (R1–R3), the domain-level maturity score for each NIST CSF function was calculated as the unweighted arithmetic mean of item scores across respondents and across items within the domain, following Equation 1. Unweighted averaging was used, rather than the weighted-average approach proposed in earlier drafts of this instrument, because no validated weighting scheme for item criticality had yet been established for this audit context; this is acknowledged as a limitation in Section 5,

$$SM = \frac{(\Sigma Si)}{n} \qquad \text{Equation (1)}$$

where SM is the domain maturity score, Si is the score of item i across all respondents who completed that item, and n is the total number of completed item-respondent observations within the domain.

Likelihood and Impact ratings used in the risk register (Section 3.4) were derived qualitatively from interview evidence and triangulated across respondents, using a 1–5 ordinal scale where 1 indicates rare/negligible, and 5 indicates near-certain/severe, consistent with common qualitative risk-matrix conventions (Abbas & Alazawi, 2026). Likelihood and Impact definitions are summarized in Table 4.

Table 4. Likelihood and Impact Rating Scale

Scale	Likelihood Descriptor	Impact Descriptor
1	Rare, no recorded occurrence	Negligible, no operational disruption
2	Unlikely, isolated occurrence	Minor limited, quickly recoverable disruption
3	Possible, occurs under specific conditions	Moderate partial operational disruption
4	Likely, recurring or structurally probable	Major significant disruption or data exposure
5	Almost certain, actively occurring or unmitigated	Severe system-wide failure or irreversible data loss

Limitations of the Legal Mapping Approach

The mapping of technical findings to specific UU PDP articles in Section 3.5 is interpretive and indicative; it identifies the statutory provisions a finding is most likely to implicate if exploited, rather than constituting a definitive legal determination of fault, which would require formal evidentiary and procedural processes beyond the scope of this audit.

The systematic alignment between NIST CSF 2.0 sub-categories and Indonesia's UU PDP (Law No. 27 of 2022) was established to bridge technical controls with legal mandates. The complete, granular cross-walk mapping, along with the required audit evidence and verbatim statutory references, is provided in Appendix A.

Result

Cybersecurity Maturity Profile

Aggregated maturity scores across the six NIST CSF 2.0 functions are presented in Figure 2 and summarized in Table 5.

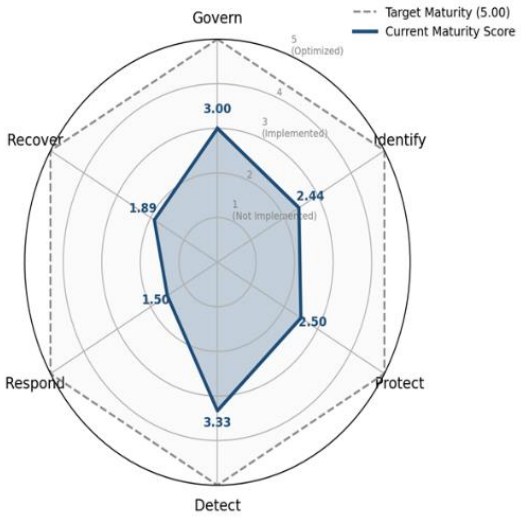


Figure 2. Cybersecurity Maturity Profile of the Six NIST CSF 2.0 Functions (Spider Chart)

As depicted in Figure 2, the solid blue line shows the hotel's current maturity score for each function on a 1–5 scale (1 = Not Implemented, 5 = Optimized and Continuously Reviewed; see Table 1 for full rubric); the dashed grey line marks the optimal target score (5.00) applied to every function. The larger the gap between the blue line and the dashed line on a given axis, the more urgent that function is for remediation. The chart highlights that Detect (3.33) and Govern (3.00) achieved scores closest to the target, while Respond (1.50) and Recover (1.89) exhibited the widest capability gaps.

Table 5 presents the same scores in tabular form, together with a qualitative maturity-status label for each function, for readers who prefer a numeric summary. Current Score is the average of all item-level interview scores within each function, rated on the 1–5 maturity rubric in Table 2 (1 = Not Implemented; 5 = Optimized and Continuously Reviewed). Maturity Status summarizes, in plain language, what the score implies about the current state of controls in that function. Domains are listed from highest to lowest maturity.

Table 5. Aggregated Maturity Scores by NIST CSF 2.0 Function

Domain	Current Score (1–5)	Maturity Status
Detect	3.33	Implemented, partially monitored
Govern	3.00	Implemented
Protect	2.50	Inconsistent to implemented
Identify	2.44	Inconsistent
Recover	1.89	Inconsistent
Respond	1.50	Largely not implemented

Detect achieved the highest relative maturity (3.33), driven primarily by consistent system-level activity logging (DE1 = 4.00), although periodic log review remains reactive rather than scheduled (DE2 = 2.67). Govern (3.00) reflects the existence of centrally issued IT security SOPs and a designated IT Officer role, though localized review at the property level remains limited. In contrast, Respond (1.50) and Recover (1.89) show the most severe capability deficits: no respondent reported prior incident-response simulation (RS2 averaged 1.00), and restore testing for backup data had never been performed (RC2 = 1.00), with site-level endpoint backup execution rated as largely unrealized (RC3 = 1.33) despite an annual capital-expenditure plan.

Gap Analysis

To prioritize domain remediation, the gap score for each NIST CSF 2.0 domain was calculated using Equation 2,

$$Gap = Target\ Score - Current\ Score \quad \text{Equation (2)}$$

where $Target\ Score$ represents the optimal score of 5.00 consistent with the maturity rubric in Table 2, and $Current\ Score$ denotes the domain average derived from Equation 1. The detailed gap values and corresponding priority rankings from P1 (Critical) to P6 (Low) are detailed in Table 6.

Respond ranks as the highest-priority remediation domain, reflecting the absence of a documented incident-response SOP at the property level and the complete absence of incident-simulation exercises. Notably, the existing organizational incident-reporting channel (escalation to the General Manager, Regional Director of Finance, Vice President, and ownership) was designed for guest- and facility-safety incidents and has not been adapted for IT/data-breach scenarios, leaving a structural gap relative to the UU PDP's incident-notification requirements.

Table 6. Gap Analysis and Remediation Priority

Domain	Current	Target	Gap	Priority
Respond	1.50	5.00	3.50	P1 (Critical)
Recover	1.89	5.00	3.11	P2 (High)
Identify	2.44	5.00	2.56	P3 (High)
Protect	2.50	5.00	2.50	P4 (Moderate)
Govern	3.00	5.00	2.00	P5 (Moderate)
Detect	3.33	5.00	1.67	P6 (Low)

Human Factor and Access Control Findings

Front-line security awareness, assessed through a ten-item Human Factor checklist administered to the Front Office Leader, yielded an average score of 2.10, the lowest aggregate score among all instrument categories. Notable findings include a lack of phishing-concept awareness (FO2 = 1.00), routine password-sharing across Front Office staff, daily workers, and on-the-job trainees (FO6 = 1.00; FO7 = 1.00), and recurring operational disruption from power loss affecting Front Office terminals when automatic backup generator activation failed (FO9 = 3.00).

Access-control findings were more heterogeneous: the Income Audit/Accounts Receivable respondent reported consistently enforced least-privilege access (average 3.25), whereas the General Cashier/Accounts Payable respondent reported broader-than-necessary access spanning Receiving, Inventory, and Front Office cashiering functions, alongside the absence of incident-reporting awareness (average 2.25). Both respondents confirmed the absence of Uninterruptible Power Supply (UPS) protection for their workstations, with backup limited to data already captured within the centralized PMS interface; locally held spreadsheet-based financial data was not subject to any backup routine.

Risk Register

Likelihood and Impact are both rated on the 1–5 ordinal scale defined in Table 4 (1 = rare/negligible, 5 = almost certain/severe). The overall Risk Score is calculated as $Score = Likelihood \times Impact$ ($maximum\ possible = 25$) and grouped into four risk categories: Score 1–6 = Low, 7–11 = Moderate, 12–15 = High, and 16–25 = Critical. The quantitative risk evaluation for the property is synthesized in Table 7, ordered from highest to lowest risk score.

Table 7. Risk Register

ID	Risk Description	Likelihood	Impact	Score	Category
R01	Inconsistent UPS coverage is causing PMS/power-dependent terminal failure during outages	4	4	16	High
R02	Endpoint and ancillary (spreadsheet) data backup failure; no restore testing performed	5	4	20	Critical
R03	Reliance on a centrally managed encryption/integration channel (Channel Manager–OTA) with no local TLS verification capability	3	4	12	High
R04	Unmanaged credential sharing and low phishing awareness among front-line staff	4	3	12	High

R02 represents the most critical exposure (Score = 20), driven by the combination of unrealized scheduled backups (RC3) and the absence of any restore-testing precedent (RC2), compounded by uncontrolled local storage of financial spreadsheet data outside the PMS backup scope (AC7). This condition, if exploited by ransomware or hardware failure, presents a high likelihood of unrecoverable

data loss. R01 (power management) and R04 (human factor/credential hygiene) both register as High, reflecting tangible, previously experienced operational disruptions (FO9) and routine, multi-party credential sharing that undermines individual accountability for system actions.

Structural Mapping to UU PDP Provisions

Table 8 maps the audit findings to the UU PDP provisions they are most likely to implicate. As noted in Section 2.3, this mapping is indicative rather than a formal legal determination. Each row links one technical finding (NIST Domain / Audit Finding) to the specific UU PDP article it could potentially trigger if left unaddressed, and explains in plain language what that would mean for the organization's legal exposure (Indicative Implication). This mapping identifies risk, not a finding of legal fault.

Table 8. Indicative Mapping of Audit Findings to UU PDP Provisions

NIST Domain	Audit Finding	Related UU PDP Article	Indicative Implication
Protect	Inconsistent UPS coverage / power-dependent system failure	Article 35	Potential failure to maintain a reliable data-processing system.
Recover	Unrealized endpoint backup; no restore testing	Article 39	Potential failure to ensure continuity of data protection.
Respond	No property-level incident-response SOP or simulation	Article 46	Potential failure to meet incident-handling and notification obligations.

If these gaps culminate in an actual data-breach event, Hotel X could face administrative sanctions under Article 57 of the UU PDP, including fines of up to 2% of annual revenue, in addition to potential civil claims and reputational damage. These exposures are presented as risk projections to inform proactive remediation, not as predictions of any pending regulatory action.

Discussion

The empirical findings detailed in Section 4 reveal deep operational vulnerabilities that extend far beyond technical glitches, providing strong support for our theoretical framework.

- **Analysis of P_1 (Subsystem Coupling):** Grounded in Socio-Technical Systems (STS) theory, the severe gap between high-level governance and localized execution illustrates a weak coupling between the technical subsystem (e.g., hardware terminals, unbacked spreadsheets, power dependencies) and the social subsystem (front-line staff and trainees). While corporate oversight ensures high maturity in structural policies (*Govern*), local operational capabilities such as disaster recovery and endpoint backup collapse because front-line personnel lack proper training and independent technical authority (evidenced by R01 and R02). When power failures or backup anomalies occur, the socio-technical loop breaks because the human actors cannot independently remediate the technical failure.
- **Analysis of P_2 (Institutional Decoupling):** Grounded in Institutional Theory (Coercive Isomorphism), the coexistence of formal compliance structures and widespread operational non-compliance (such as routine multi-party credential sharing, FO6/FO7 = 1.00) confirms a state of structural decoupling. External pressures stemming from Indonesia's Personal Data Protection Law (UU PDP No. 27/2022) successfully compel the organization to adopt ceremonial policies. However, daily operational routines at the front-line layer continue to prioritize workflow convenience over data security, meaning regulatory coercion drives documentary compliance rather than true behavioral changes.

When evaluated against existing literature, these findings refine our understanding of cybersecurity postures in the hospitality sector. While prior studies by Karadayi-Usta (2024) and Pipyros and Liasidou (2025) largely focused on high-level managerial risk perceptions or general risk assessments, our multi-

layer approach exposes the exact friction points in hybrid cloud-local PMS architectures, extending the insights of Bernardo et al. (2025). Furthermore, unlike standard GDPR cross-sector analyses (e.g., Voigt & Von dem Bussche, 2017), our findings demonstrate how physical infrastructure deficiencies such as unbacked local financial spreadsheets and inconsistent UPS coverage translate directly into statutory violations of data continuity and protection mandates under Articles 35 and 39 of the UU PDP Law.

To bridge the gap between identified risks (such as R02's critical score of 20 and R01/R04's high scores) and regulatory compliance under Articles 35, 39, and 46, organizations managing hybrid hotel properties must implement tiered, structural interventions rather than temporary fixes:

- **Respond / Recover Interventions (P1–P2):** Establishing property-level incident response capabilities aligned with UU PDP 3x24-hour notification timelines.
- **Power Resilience Upgrades (R01):** Standardizing UPS coverage with Automated Voltage Regulation across all front-line terminals, moving beyond server-room-only protections.
- **Endpoint & Backup Security (R02):** Deploying EDR agents, automated AES-256 encrypted NAS backups, and periodic restore testing that explicitly encompasses local spreadsheet-based financial records.
- **Human Factor & Access Hygiene (R04):** Eradicating unmanaged credential sharing through role-based access control (RBAC) and conducting phishing awareness simulations for front-line staff and trainees.

Conclusion

This study successfully developed and demonstrated a hybrid cybersecurity compliance audit framework tailored for on-premises hotel Property Management Systems (PMS) integrated with cloud-based channels, bridging NIST CSF 2.0 technical controls with Indonesia's Personal Data Protection (UU PDP) Law No. 27 of 2022.

Utilizing DSR methodology and multi-layer assessment at Hotel X, findings confirm that while high-level governance achieved moderate maturity (3.00), local technical execution and incident response lagged substantially (1.50). Furthermore, the study verified two core theoretical propositions: subsystem coupling (P_1) failures in power/backups and institutional decoupling (P_2) through ceremonial compliance versus front-line non-compliance.

Through a rigorous cross-walk mapping matrix and qualitative risk prioritization, the research translated physical infrastructure gaps and human factor vulnerabilities into explicit statutory legal exposures under Articles 35, 39, and 46 of the UU PDP Law. Future work should focus on scaling and validating this audit instrument across broader multi-property portfolios.

References

Abbas, A. S., & Alazawi, S. A. H. (2026). Risk evaluation for bank information security management in network environment considering ISO/IEC 27001 and ISO/IEC 27005. *AIP Conference Proceedings*, *3408*(1), 020012. https://doi.org/10.1063/5.0329787

Badawi, S. A., Takruri, M., Salameh, K., Guessoum, D., ElBadawi, I., & Al-Qaisi, A. (2026). Data governance and security assurance in ISO27001 programs: A context study on quality and compliance in Middle Eastern organizations. *Applied Mathematics & Information Sciences*, *20*(1), 253–265. https://doi.org/10.18576/amis/200117

Bernardo, L., Malta, S., & Magalhães, J. (2025). An evaluation framework for cybersecurity maturity aligned with the NIST CSF. Electronics, 14(7), 1364. https://doi.org/10.3390/electronics14071364

Brezavšček, A., & Baggia, A. (2025). Recent trends in information and cyber security maturity assessment: A systematic literature review. *Systems*, *13*(1), 52. https://doi.org/10.3390/systems13010052

Büyüközkan, G., & Güler, M. (2025). Cybersecurity maturity model: Systematic literature review and a proposed model. *Technological Forecasting and Social Change*, *213*, 123996. https://doi.org/10.1016/j.techfore.2025.123996

Campoverde-Molina, M., & Luján-Mora, S. (2025). Cybersecurity in smart agriculture: A systematic literature review. *Computers & Security*, *150*, 104284. https://doi.org/10.1016/j.cose.2024.104284

Casaril, F., & Galletta, L. (2025). Developing security metrics for space systems: A study considering the NIST Cybersecurity Framework 2.0 and the NIS2. *International Journal of Critical Infrastructure Protection*, *51*, 100805. https://doi.org/10.1016/j.ijcip.2025.100805

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

Demir, M., & Demir, Ş. Ş. (2025). The relationship between technology investments, innovation strategies, and competitive performance in the hospitality industry: A mixed methods approach. International *Journal of Hospitality Management*, *128*, 104151. https://doi.org/10.1016/j.ijhm.2025.104151

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

Kim, H. B., Lee, D. S., & Ham, S. (2013). Impact of hotel information security on system reliability. *International Journal of Hospitality Management*, *35*, 369–379. https://doi.org/10.1016/j.ijhm.2012.06.002

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1) (NIST Cybersecurity White Paper CSWP 4). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST Special Publication SP 1299). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

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

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. *Sekretariat Negara*.

Sari, I. P., Ramadhan, A., & Hermawan, B. (2023). Analisis Pasal 56 dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dari perspektif kepastian hukum. *Jurnal Hukum Privasi*, *2*(1), 45–58.

Tarumingkeng, R. C. (2022). Analisis risiko siber dan tata kelola keamanan informasi pada sektor industri strategis. *Penerbit Buku Ilmiah*.

Cobanoglu, C., Dogan, S., Berezina, K., & Collins, G. (2021). Hospitality and tourism information technology. *USF M3 Publishing*, LLC. https://doi.org/10.5038/9781732127593

Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. *Springer International Publishing*. https://doi.org/10.1007/978-3-319-57959-7

Wibowo, A., Sofyan, M., & Budiman, A. (2023). Urgensi penguatan regulasi pelindungan data dan keamanan siber di Indonesia terhadap ancaman hacking dalam sistem pemerintahan berbasis elektronik. *Jurnal Keamanan Siber Nasional*, *5*(2), 112–128.

How to cite:

Sudana, I. M., Handaga, B., & Wantoro, J. (2026). Hybrid Cybersecurity Compliance Audit Framework for an On-Premise Hotel Property Management System: Mapping NIST CSF 2.0 Controls to Indonesia's Personal Data Protection Law. *Jurnal Sistem Informasi (Journal of Information System)*, *22*(2), 64–80.

Appendices

Appendix A
Detailed Cross-Walk Mapping Matrix (NIST CSF 2.0 Sub-Categories to UU PDP Law)

NIST CSF 2.0 Function	Sub-Category ID	NIST CSF 2.0 Sub-Category Description	UU PDP Law (No. 27/2022)	Statutory Mandate / Requirement Summary	Required Audit Evidence
PROTECT (PR)	PR.AC-01	Identities and credentials are authenticated and managed.	Article 35 (Paragraph 1 & 2)	Obligation to protect personal data from unauthorized access through secure authentication mechanisms.	Active user accounts list in PMS vs. active front-line staff roster, password complexity policy, multi-factor authentication (MFA) configuration logs.
PROTECT (PR)	PR.DS-01	Data-at-rest is protected against unauthorized access and disclosure.	Article 35 (Paragraph 1) & Article 39	Duty to implement technical safeguards (encryption/access restriction) for personal data storage.	Database encryption status reports, physical server room access logs, local NAS backup encryption configurations.
PROTECT (PR)	PR.DS-02	Data-in-transit is protected against unauthorized access and disclosure.	Article 35 (Paragraph 1) & Article 39	Ensuring data security during transmission across internal networks and external cloud integrations (OTAs).	Channel Manager API encryption protocols (TLS/SSL certificates), firewall rule sets, network topology diagrams.
PROTECT (PR)	PR.DS-11	Backups of data are created, protected, and tested.	Article 39 (Paragraph 1 & 2)	Obligation to implement security measures to prevent loss or unauthorized alteration of personal data, including backup management.	Backup execution logs, off-site backup schedules, hardware redundancy inventory (UPS/AVR status), and restoration test reports.
DETECT (DE)	DE.AE-02	Anomalous activity is detected across the information system.	Article 46 (Paragraph 1)	Obligation to monitor systems for security incidents and anomalies that may compromise personal data.	System audit trails, PMS access logs, error logs, and endpoint detection/monitoring configurations.
DETECT (DE)	DE.CM-01	Networks and physical environments	Article 35 & Article 46	Continuous monitoring of processing	Physical inspection of server rooms, CCTV logs covering

NIST CSF 2.0 Function	Sub-Category ID	NIST CSF 2.0 Sub-Category Description	UU PDP Law (No. 27/2022)	Statutory Mandate / Requirement Summary	Required Audit Evidence
		are monitored to find potentially unauthorized activities.		systems to detect vulnerabilities, unauthorized nodes, or breaches.	terminal access, and network monitoring tool configurations.
RESPOND / GOVERN	RC/GV	Incident response and organizational governance procedures are established.	Article 46 (Paragraph 2) & Article 57	Mandatory notification protocols for data breaches (within 3x24 hours) and administrative sanctions for non-compliance.	Incident response SOP documents, data breach notification templates, and records of past security incident handling.