International Journal of Multidisciplinary Research and Growth Evaluation.

Digital Technology Readiness for Hotel Business Takeovers in Malaysia: A Due Diligence Framework

Mohd Zahiruddin Zuhri [1*], Mohd Nadzri Jaafar [2]
[1-2] Faculty of Built Environment and Surveying, Universiti Teknologi Malaysia, Johor Bahru, Johor, Malaysia

* Corresponding Author: **Mohd Zahiruddin Zuhri**

Article Info

ISSN (Online): 2582-7138
Volume: 07
Issue: 06
Received: 24-08-2026
Accepted: 26-09-2026
Published: 28-10-2026
Page No: 112-118

Abstract
Technology is central to hotel operations, but it is often assessed only after a business takeover has been completed. This paper develops a conceptual decision-support framework for evaluating digital technology readiness before a hotel business takeover in Malaysia. An integrative review of hospitality technology, information systems, digital transformation, cybersecurity, privacy, payment security and business continuity literature were used to identify eight assessment dimensions. The framework combines a five-level readiness scale, a Digital Technology Readiness Index (DTRI) and a separate review of critical technology risks that should not be concealed by an overall score. It also links the evidence collected during due diligence with takeover decisions and transition planning. The proposed framework offers a transparent basis for comparing hotel targets, estimating improvement requirements and assigning responsibility for technology risks. As a conceptual model, it requires expert review and case-based validation before sector-wide application.

DOI: https://doi.org/10.54660/.IJMRGE.2026.7.6.112-118

Keywords: Cybersecurity, digital due diligence, hotel takeover, information systems, technology readiness

1. Introduction

Technology is now embedded in almost every stage of a hotel stay, from online discovery and reservation to identity verification, room access, payment, service recovery and post-stay relationship management (R. Leung, 2019; Zuhri *et al*., 2026) [12, 23]. The same infrastructure also supports forecasting, revenue optimization, labour scheduling, financial reporting and owner oversight. Consequently, the transfer of a hotel business includes a less visible digital estate made up of applications, interfaces, databases, licenses, vendor contracts, credentials, devices and operating knowledge (Yu *et al*., 2025) [22]. A takeover can be legally complete while the digital operating model remains technically fragile.

The risk is especially material during the interval between signing and operational handover. Systems may be owned by the vendor, franchisor, operator or a third-party platform, interfaces may rely on undocumented scripts and customer records may contain incomplete consent histories. Privileged accounts may remain with departing personnel and legacy applications may be unsupported. If these dependencies are identified only after completion, the acquirer may face interrupted room inventory, rate parity failures, payment exposure, inaccurate management information or emergency replacement costs.

Malaysian hotel-takeover research has already established technology as one of the decision dimensions considered by industry participants (Zuhri *et al*., 2026) [23]. However, a factor-level priority does not tell an acquirer what evidence to request, how to test readiness, or when a technology weakness should stop or reprice a transaction. This paper addresses that implementation gap. It does not reanalyze the respondents, matrices or numerical results reported in (Zuhri *et al*., 2026) [23]. Instead, it develops a distinct technical artefact for pre takeover assessment.

This paper has three objectives. First, it identifies the key technology components that should be assessed before a hotel business takeover. Second, it organises these components into a structured and auditable due diligence framework. Finally, it proposes a

readiness index to support managerial decision-making while highlighting critical risks that should take priority over the overall score.

Th paper makes both practical and conceptual contributions. In practical terms, it converts technology into specific matters that can be supported by documents, reviewed and assessed. Conceptually, it connects hospitality technology research with information systems quality, organisational readiness, cybersecurity governance and business continuity. The framework is intended for hotel owners, investors, asset managers, operators, technology advisers and teams involved in hotel business takeovers in Malaysia.

2. Technology Risk in Hotel Business Takeovers

2.1. The Hotel as a Digital Service Ecosystem

A contemporary hotel is not supported by a single information system. The property management system (PMS) exchanges data with the central reservation system, channel manager, point-of-sale platform, payment gateway, accounting system, customer relationship management (CRM) platform, revenue-management system, door-lock solution and business intelligence tools (Law *et al*., 2014) [9]. Interfaces with online travel agencies, brand platforms and loyalty programmes extend the boundary beyond the property. According Buhalis & Leung (2018), describe smart hospitality in terms of interconnectivity and interoperability, while later work emphasises that digital performance depends on the combined alignment of technologies, organisational competencies and operating processes (Busulwa *et al*., 2022) [2].

This ecosystem view changes the unit of due diligence. Reviewing the age of the PMS alone is insufficient (Gessa *et al*., 2026) [4]. The acquirer must understand the architecture, data flows, interface dependencies, support arrangements and failure modes of the whole digital service chain. A modern front-end can still depend on unsupported middleware, untested backups or a contract that cannot be assigned to the buyer.

2.2. Why Takeover Conditions Amplify Technology Risk

Takeovers create simultaneous technical, contractual and organisational change. User accounts must be revoked or transferred, domain names and digital storefronts must be reassigned and payment merchant arrangements may changed. Historic data must be migrated or retained and operational teams may move to a new reporting structure. These activities occur under fixed transaction dates and with limited tolerance for service interruption. The risk is therefore not only whether a system performs today, but whether it can continue to perform under a change of control (Hong *et al*., 2024) [5].

Technology risk also affects valuation. Remediation may require licence buyouts, interface redevelopment, network replacement, specialist consultants, cybersecurity improvements, staff training or temporary parallel systems. Some costs are visible capital items, whereas others appear as lower conversion, higher commissions, revenue leakage, manual work or delayed management reporting (Lei *et al*., 2021) [10]. A due diligence model should therefore link technical condition to price adjustment, conditions precedent and the first 100 days transition plan.

2.3. Malaysian Governance Context

Hotels process identity, contact, stay-history and payment-related information. In Malaysia, handling of personal data must be assessed against the Personal Data Protection Act 2010 (Act 709) and subsequent amendments (*Personal Data Protection Act 2010 [Act 709] • Personal Data Protection*, n.d.) [15]. Cybersecurity governance should also consider the national direction represented by the Cyber Security Act 2024 (Act 854), where applicable (Setasign, 2024) [17], while payment environments should be assessed against applicable PCI DSS obligations (Gessa *et al*., 2026) [4]. These sources do not replace transaction specific legal advice, but they establish why data ownership, access control, incident response and vendor accountability are core takeover questions rather than optional technical checks (Rushmore, 2003) [16].

3. Conceptual Foundations

The framework draws on four complementary lenses. First, the technology–organisation–environment (TOE) perspective treats adoption and readiness as the result of technical characteristics, organisational capacity and external conditions (D. Leung *et al*., 2015) [11]. This is useful because the same platform can be acquisition-ready in a well-governed hotel and high-risk in a property without skilled staff or transferable vendor support. Second, the DeLone - McLean information systems success model distinguishes system quality, information quality and service quality (Delone & Mclean, n.d.). These constructs direct attention to reliability, data integrity and support rather than product labels alone.

Third, digital-transformation research treats technology change as an organisational transformation rather than a software purchase (Busulwa *et al*., 2022; Vial, 2019) [2, 20]. This lens informs assessment of ownership, skills, change capacity and expected value. Fourth, recognised control frameworks provide operational tests. NIST CSF 2.0 organises cybersecurity around governance, identification, protection, detection, response and recovery (Institute of Standards, 2024) [6], ISO/IEC 27001:2022 provides an information-security management-system baseline (*ISO/IEC 27001:2022 - Information Security Management Systems*, n.d.), ISO 22301:2019 informs continuity and recovery (ISO 22301:2019(En), Security and Resilience - Business Continuity Management Systems -Requirements, n.d.), and PCI DSS v4.0.1 addresses cardholder-data environments according PCI Security Standards Council, Payment Card Industry Data Security Standard: Requirements and Testing Procedures, Version 4.0.1, June 2024 (n.d.).

Table 1: Conceptual lenses and their role in the proposed framework

Lens	Application in the framework
TOE perspective	Can the technology operate within the organisation and its external environment? Assesses architecture together with skills, vendors, contracts and regulatory constraints (D. Leung *et al*., 2015; Tornatzky & Fleischer, 1990) [11, 19].
IS success	Are systems reliable, usable and capable of producing trustworthy information? Adds system quality, information quality and service/support evidence (Delone & Mclean, n.d.).
Digital transformation	Can the acquirer convert technology capability into operating value? Adds leadership, competence, change effort and benefit realisation considerations (Busulwa *et al*., 2022; Gessa *et al*., 2026; Vial, 2019) [2, 4, 20]
Security and continuity	Can services and data remain protected and recoverable? Adds governance, access, testing, incident response, backup and recovery controls (Institute of Standards, 2024; *ISO 22301:2019(En), Security and Resilience — Business Continuity Management Systems — Requirements*, n.d.; *ISO/IEC 27001:2022 - Information Security Management Systems*, n.d.; *PCI DSS 4.0.1 Requirements Overview	PDF	Payment Card Industry Data Security Standard	Security Engineering*, n.d.).

Note. Synthesised by the author from the cited theories and standards.

4. Method

This study uses an integrative conceptual review, a method suited to combining established research streams and producing a new framework for an applied problem webster (Snyder, 2019; Webster & Watson, 2002) [18, 21]. The review was problem driven rather than a systematic review and therefore does not claim exhaustive coverage or PRISMA-style record counts. Sources were selected for their direct relevance to hotel digital ecosystems, technology adoption and capability, information systems quality, cybersecurity, privacy, payment security and business continuity.

The synthesis proceeded in four stages. First, recurring technology dependencies in hotel operations were identified from hospitality and digital transformation literature (Buhalis & Leung, 2018; Busulwa *et al*., 2022; Gessa *et al*., 2026; D. Leung *et al*., 2015; Vial, 2019) [1, 2, 4, 11, 20]. Second, those dependencies were reframed as takeover risks by asking whether each asset, right, contract, dataset and capability could be verified and transferred. Third, the risks were grouped into mutually distinct but operationally connected dimensions. Fourth, evidence requirements, maturity anchors and red flags were added so that the conceptual categories could support a consistent pre-acquisition review.

No primary survey, interview or property level dataset was used. The DTRI equation and risk bands are design propositions, not statistically estimated cut-offs. They are offered to make judgement explicit and comparable as empirical calibration remains a future research task.

5. Proposed Digital Technology Readiness Framework

5.1. Eight Assessment Dimensions

The framework contains eight dimensions. Each dimension is defined by the operational outcome that should survive the ownership transition, the evidence required to support a score and the main transaction exposure if the dimension is weak.

Table 2: Digital technology readiness dimensions for hotel takeovers

Dimension	Main Due Diligence Test
Core hotel systems	The assessment examines whether the main hotel systems, including the property management system, point-of-sale system, reservation system, financial system, procurement system and workforce management system, remain suitable and operational. The review should consider the system versions, licences, vendor support, maintenance records and previous service interruptions.
Integration and interoperability	This dimension examines how effectively the hotel systems are connected and whether information can be transferred accurately between them. The assessment should identify system interfaces, recurring errors, duplicated processes and any dependence on a single system or service provider.
Data ownership, quality and migration	The assessment determines whether the hotel has the legal right to access, transfer and continue using its operational and guest data after the takeover. It should also examine the completeness and accuracy of the data, its retention arrangements and the feasibility of transferring it to the buyer's systems.
Cybersecurity and access control	This dimension evaluates the measures used to protect the hotel's systems and information. The review should cover user access, password controls, system monitoring, reported security incidents, data backups and recovery procedures. Particular attention should be given to unresolved weaknesses that may be transferred to the new owner.
Revenue management and analytics	The assessment examines whether the hotel's forecasting, pricing and performance reporting systems provide reliable information for managerial decisions. Forecast results, pricing adjustments, performance indicators and management reports should be compared with actual hotel performance.
Digital distribution and customer relationship management	This dimension examines the hotel's control over its website, domain name, online travel agency accounts, channel manager, customer database and digital marketing assets. The review should confirm account ownership, contractual arrangements, access rights and the ability to continue these services after the takeover.
Guest-facing services and payments	The assessment considers the condition, reliability and security of digital services used by hotel guests. These include Wi-Fi, mobile applications, self-service kiosks, electronic door locks, contactless services and payment systems. Any weaknesses that may affect guest experience, safety or payment security should be identified.
Transformation cost, capability and readiness	This dimension determines whether the buyer has sufficient financial resources, employees, technical skills and implementation plans to complete the technology transition. The assessment should consider the estimated cost, vendor agreements, staff training, implementation schedule and dependence on existing hotel employees.

Note. The dimensions constitute the proposed DTRI model. Evidence examples are indicative and should be adjusted to the transaction perimeter

5.2. Maturity Scale

Assessors assign one maturity score to each dimension after reviewing evidence and testing selected controls. The score represents demonstrated takeover readiness, not managerial confidence or vendor assurances. Where evidence is missing, the assessor should not infer maturity from system age or brand reputation.

Table 3: Five-level maturity scale

No.	Score and readiness level	Assessment and implication for the takeover decision
1	Critical	The technology is obsolete, no longer supported or exposed to serious security weaknesses. Important documents and system records are also incomplete or unavailable. This condition may prevent the takeover from proceeding unless the identified problems are resolved or a replacement plan is prepared.
2	Weak	Several weaknesses exist in the systems, controls and supporting documents. Considerable cost and effort may be required, while the transfer of systems, data or licences to the buyer remains uncertain. The buyer should consider appropriate measures, including a price adjustment, additional warranties or early corrective action.
3	Acceptable with improvements	The main hotel operations can continue after the takeover, although several improvements and additional investments are required. The takeover may proceed if the required work, estimated cost, responsible parties and implementation period are clearly identified.
4	Strong	The technology is supported, properly documented and generally transferable to the buyer. Only minor weaknesses remain, and these are unlikely to significantly interrupt hotel operations. Any outstanding improvements should be monitored during the transition period.
5	Ready for takeover	The technology is secure, properly maintained and supported by complete documentation. The systems, data, licences and contractual arrangements can be transferred to the buyer, while backup and recovery procedures have been tested. The technology transition can therefore proceed according to the agreed takeover plan.

5.3. Digital Technology Readiness Index

An equal weight baseline is recommended until empirical research establishes defensible differential weights. Equal weighting is transparent, avoids false precision and makes the model usable across independent, branded and managed hotels. Let s_i denote the score for dimension i, where i = 1,…,8 and $s_i \in \{1,2,3,4,5\}$. The proposed index is given in equation (1):

$$\text{DTRI} = \left(\frac{\sum s_i}{40}\right) \times 100 \quad (1)$$

The denominator of 40 is the maximum total score across eight dimensions. The conversion produces a 0–100 reporting scale, although the practical minimum under the five-level rubric is 20. The score should be reported with the dimension profile and evidence limitations; a single number must not replace professional judgement.

Table 4: Proposed DTRI interpretation bands

DTRI score and readiness level	Implication for the takeover decision
20–39 – Critical risk	The existing technology is not sufficiently ready to support the hotel business takeover and may cause serious operational disruption. The takeover should not rely on the existing systems unless the major weaknesses are corrected or a replacement plan is prepared before the transition.
40–59 – High risk	Significant weaknesses remain in the systems, controls or supporting documents. The decision to proceed should be supported by a clear improvement plan that identifies the required cost, responsibilities, implementation period and appropriate protection for the buyer.
60–74 – Moderate readiness	The technology is generally able to support the takeover, although several improvements are still required. A funded implementation plan should be prepared, with specific responsibilities, completion targets and system testing requirements.
75–89 – Substantially ready	The technology is largely ready to support the takeover, with only minor weaknesses remaining. Before completing the takeover, the buyer should confirm the transfer of contracts, licences and system access, as well as the effectiveness of backup and recovery procedures.
90–100 – Ready for takeover	The technology is well prepared to support the takeover. The systems are supported, documented, secure and transferable to the buyer. Only final verification and continued monitoring are required during the transition period.

Note. Bands are proposed design parameters and have not yet been empirically calibrated.

5.4. Critical Technology Risks Requiring Separate Consideration

Although the DTRI provides an overall indication of technology readiness, the final assessment should not be based solely on the total score. A satisfactory score in several dimensions may conceal a serious weakness in another dimension. Therefore, critical technology risks should be assessed separately before a hotel is considered ready for takeover.

Particular attention is required when the ownership or transfer of guest and employee data cannot be confirmed. Similar concerns arise when an important hotel system, such as the property management, reservation, payment, electronic lock or financial system, is no longer supported or cannot be transferred to the buyer. The sharing of administrator access, the continued access of departing employees and the absence of effective procedures for removing access may also expose the buyer to operational and security risks.

Other critical concerns include the absence of tested backup and recovery procedures, unresolved cybersecurity incidents, weaknesses in the payment environment and uncertainty over the transfer of important vendor, franchisor or hotel operator agreements. Where any of these conditions are identified, the hotel should not automatically be considered ready for takeover, even when its overall DTRI score is high.

Decision makers should first examine the seriousness of the weakness, its possible effect on hotel operations and the cost and time required to address it. The takeover may proceed when the issue has been corrected, formally accepted by the parties or managed through an appropriate contractual and transition arrangement. This separate assessment reduces the possibility that a serious technology weakness will be overlooked within the overall readiness score.

6. Operational Due Diligence Procedure

The framework should be used as a controlled workflow rather than a one-off

Table 5: Five-phase due diligence workflow

Phase	Main activity and expected outcome
1. Determine the scope	This phase identifies the properties, business entities, hotel brands, operators, shared services and technology systems included in the assessment. The responsibilities of the parties and the expected takeover date should also be clarified. The outcome is a clearly defined assessment scope covering all systems that are important to hotel operations.
2. Collect supporting information	Relevant information is collected to understand the existing condition of the hotel's technology. This includes system inventories, licences, contracts, system diagrams, access records, operational logs, data records, technology costs and previous incidents. Any missing, incomplete or outdated information should be identified for further review.
3. Verify the systems and information	The information provided by the seller is verified through appropriate reviews and testing. This may include checking data accuracy, system interfaces, user access, data export capabilities, backup and recovery procedures and vendor support. The purpose is to determine whether the systems can continue operating under the new ownership.
4. Assess technology readiness	Each technology dimension is assessed using the proposed scoring scale, followed by the calculation of the DTRI. Critical risks should be considered separately, and the reasons for each score should be documented. The results provide an overall view of the hotel's technology readiness and support the decision to proceed, undertake improvements, continue negotiations or postpone the takeover.
5. Prepare the transition plan	The findings are translated into a practical transition plan. The plan should identify the required improvements, estimated budget, responsible parties, implementation period, transfer of contracts and licences, changes to system access and staff training requirements. This ensures that the remaining technology risks are addressed during and after the takeover.

6.1. Evidence Discipline

Three evidence rules improve consistency. First, documentary evidence should be corroborated by observation or testing where the control is material. A backup policy, for example, is weaker evidence than a successful restoration test. Second, evidence should be transaction-specific: a group-level certification does not automatically demonstrate that the target property is within scope. Third, the score rationale should distinguish absence of control from absence of evidence. Both increase acquisition risk, but they require different follow-up actions.

6.2. Linking Findings to Transaction Mechanisms

A due diligence finding is useful only when it changes a decision or an action. Critical weaknesses may be translated into conditions precedent, specific warranties, indemnities, escrow or price adjustment. Moderate gaps may be placed in a costed integration budget and first 100-day plan. Lower-risk issues may be tracked as post-completion optimisation. This linkage prevents technical observations from becoming detached appendices that do not influence the investment case.

6.3. Illustrative Application

Table 6 demonstrates the calculation for a hypothetical urban hotel. The values are not observations from a real property and are included only to show how the model behaves. The hypothetical hotel has a modern distribution front end but weak integration documentation, data-transfer evidence, cybersecurity controls and transition capability.

Table 6: Hypothetical DTRI application

Dimension	Illustrative score and priority
Core hotel systems	Score 3. Confirm upgrade cost and cutover window.
Integration and interoperability	Score 2. Document, test and place vendor support under contract.
Data ownership, quality and migration	Score 2. Complete legal review and trial migration.
Cybersecurity and access control	Score 2. Treat as a red-flag workstream before completion.
Revenue management and analytics	Score 3. Standardizes governance and validate reports.
Digital distribution and CRM	Score 4. Complete novation and credential rotation.
Guest-facing services and payments	Score 3. Validate scope and vendor support.
Transformation cost, capability and readiness	Score 2. Create funded plan and appoint accountable lead.

Note. Illustrative score: $\Sigma s_i = 21$; DTRI = (21/40) × 100 = 52.5, indicating high risk. A cybersecurity red flag would override the aggregate band until resolved.

7. Discussion

7.1. Theoretical Contribution

The framework advances hotel-takeover decision support in three ways. First, it changes technology from a broad decision factor into a structured capability profile. Second, it joins system quality and interoperability with organisational readiness and external constraints, consistent with TOE and digital transformation research. Third, it separates compensatory scoring from non-compensatory risk. This is important because conventional weighted averages allow a high score in distribution or analytics to offset an unacceptable weakness in data rights, recovery or privileged access, even though the latter may threaten the transaction itself.

The framework also clarifies the boundary between an adoption model and an acquisition-readiness model. Adoption studies ask whether a hotel is likely to implement or continue using a technology (D. Leung *et al*., 2015) [11]. Acquisition readiness asks whether the buyer can lawfully control, securely operate, economically sustain and reliably

transition the digital capability at a defined date. The difference introduces transferability, evidence quality, cutover risk and contractual dependency as central constructs.

7.2. Managerial Implications

For acquirers, the DTRI creates a repeatable structure for comparing targets and testing investment assumptions. For sellers, it provides a preparation checklist that can reduce uncertainty and improve data-room quality. Operators and vendors can use the evidence catalogue to identify the interfaces, licences and support commitments that require novation. Lenders and investment committees can use the dimension profile to distinguish maintenance expenditure from mandatory transaction remediation.

The equal-weight baseline should not prevent deal-specific sensitivity analysis. A full-service branded hotel with extensive interfaces may place more emphasis on integration and brand-platform continuity; an independent limited-service property may emphasise distribution control and internal capability. Any alternative weights should be documented before scoring to avoid adjusting the model after weaknesses become visible. Red flags should remain non-compensatory regardless of weighting.

7.3. Fit with Engineering and Technology Research

Although hotel takeovers are commercial transactions, the proposed contribution is technological: it specifies an information-systems assessment architecture, measurable maturity anchors, control evidence and a decision rule. This technical framing aligns the paper with an engineering-and-technology readership interested in systems integration, risk, cybersecurity, data governance and operational resilience. The hospitality setting functions as a complex service-system application rather than as a purely financial case.

8. Limitations and Future Validation

The framework has four limitations. First, it is conceptual and has not been tested for inter-rater reliability, predictive validity or association with post-takeover performance. Second, the equal weights and interpretation bands are design choices rather than parameters estimated from Malaysian transactions. Third, hotel business models differ in scale, ownership, brand affiliation and outsourcing, so some evidence items may not apply uniformly. Fourth, standards and legal obligations evolve; each assessment must use requirements current at the transaction date and obtain qualified legal or compliance advice where necessary.

Future research should proceed in stages. A Malaysian Delphi panel of hotel owners, operators, technology specialists, transaction advisers and regulators can refine content validity and red flags. A multi-case study can test feasibility and evidence availability across independent and branded hotels. A larger study can then examine inter-rater reliability, construct structure and criterion validity against outcomes such as cutover disruption, unplanned technology expenditure, security incidents and time to stabilisation. If differential importance is supported, AHP or another multi-criteria method may subsequently estimate weights without recycling the dataset used in (Zuhri *et al*., 2026) [23].

9. Conclusion

Hotel business takeovers transfer a digital operating system as surely as they transfer rooms, contracts and physical assets. Yet technology is frequently treated as a generic checklist item or deferred to post-completion integration. The proposed framework makes digital readiness visible through eight dimensions, a five-level maturity scale, an auditable DTRI calculation and non-compensatory red flags. Its principal value is not the production of a single score, but the disciplined connection between evidence, risk, transaction terms and transition action.

For Malaysian hotel transactions, the framework offers a practical starting point for identifying whether systems, data, controls, contracts and capabilities can survive a change of ownership. It is deliberately presented as a testable decision-support artefact. Empirical validation is the next step before the model is used as a standardised benchmark across the sector.

Thank-You Note

The authors acknowledge the contributions of researchers whose work on hospitality technology, information systems, digital transformation and technology risk management informed the development of this conceptual framework.

References

1. Buhalis D, Leung R. Smart hospitality—Interconnectivity and interoperability towards an ecosystem. International Journal of Hospitality Management. 2018;71:41-50. doi:10.1016/J.IJHM.2017.11.011
2. Busulwa R, Pickering M, Mao I. Digital transformation and hospitality management competencies: Toward an integrative framework. International Journal of Hospitality Management. 2022;102:103132. doi:10.1016/j.ijhm.2021.103132
3. Delone, W. H., & Mclean, E. R. (n.d.). Sloan Management Review, and others. In Communications of the ACM. DATABASE. Han>aril Business Review (Vol. 19).
4. Gessa A, Jiménez-Jiménez A, Nemer R. Leveraging digital technology to improve hotel performance: a systematic literature review. Information Technology & Tourism. 2026;28(2). doi:10.1007/s40558-026-00399-7
5. Hong E, Shin JK, Zou H. Cross-border mergers and acquisitions from emerging economy firms: a new channel for technology augmentation. International Journal of Development Issues. 2024;23(2):282-303. doi:10.1108/IJDI-03-2023-0083
6. Institute of Standards N. The NIST Cybersecurity Framework (CSF) 2.0. 2024. doi:10.6028/NIST.CSWP.29
7. ISO 22301:2019(en), Security and resilience — Business continuity management systems — Requirements. (n.d.). Retrieved October 4, 2026, from https://www.iso.org/obp/ui/en/#iso:std:iso:22301:ed-2:v1:en
8. ISO/IEC 27001:2022 - Information security management systems. (n.d.). Retrieved October 4, 2026, from https://www.iso.org/standard/27001
9. Law R, Buhalis D, Cobanoglu C. Progress on information and communication technologies in hospitality and tourism. International Journal of Contemporary Hospitality Management. 2014;26(5):727-750. doi:10.1108/IJCHM-08-2013-0367

10. Lei, C., Hossain, M. S., Mostafiz, M. I., & Khalifa, G. S. A. (2021). Factors determining employee career success in the Chinese hotel industry: A perspective of Job-Demand Resources theory. Journal of Hospitality and Tourism Management, 48(September 2020), 301–311. https://doi.org/10.1016/j.jhtm.2021.07.001
11. Leung, D., Lo, A., Hoc, L., Fong, N., & Law, R. (2015). Applying the Technology-Organization-Environment framework to explore ICT initial and continued adoption: An exploratory study of an independent hotel in Hong Kong. https://doi.org/10.1080/02508281.2015.1090152
12. Leung R. Smart hospitality: Taiwan hotel stakeholder perspectives. Tourism Review. 2019;74(1):50-62. doi:10.1108/TR-09-2017-0149
13. PCI DSS 4.0.1 Requirements Overview | PDF | Payment Card Industry Data Security Standard | Security Engineering. (n.d.). Retrieved October 4, 2026, from https://www.scribd.com/document/744850938/PCI-DSS-v4-0-1
14. PCI Security Standards Council, Payment Card Industry Data Security Standard: Requirements and Testing Procedures, Version 4.0.1, June 2024 - Search. (n.d.). Retrieved October 4, 2026, from https://www.bing.com/search?q=PCI%20Security%20Standards%20Council%2C%20Payment%20Card%20Industry%20Data%20Security%20Standard%3A%20Requirements%20and%20Testing%20Procedures%2C%20Version%204.0.1%2C%20June%202024&qs=n&form=QBRE&sp=-1&ghc=1&lq=0&pq=pci%20security%20standards%20council%2C%20payment%20card%20industry%20data%20security%20standard%3A%20requirements%20and%20testing%20procedures%2C%20version%204.0.1%2C%20june%202024&sc=12-139&sk=&cvid=EE665C4939E84BC59B2FEEA2882E55AE
15. Personal Data Protection Act 2010 [Act 709] • Personal Data Protection. (n.d.). Retrieved October 4, 2026, from https://www.pdp.gov.my/ppdpv1/en/akta/pdp-act-2010-en/
16. Rushmore S. Hotel Management Takeover - A successful transition is like merging onto a freeway; you can do it smoothly and easily or you can jet into traffic without looking and the results can be immediate, disastrous, and cause a lasting effect. Hospitality.Net; 2003. Available from: https://www.hospitalitynet.org/opinion/4017975.html
17. Setasign. LAWS OF MALAYSIA Act 854 CYBER SECURITY ACT 2024. n.d.
18. Snyder H. Literature review as a research methodology: An overview and guidelines. Journal of Business Research. 2019;104:333-339. doi:10.1016/J.JBUSRES.2019.07.039
19. Tornatzky LG, Fleischer, Mitchell. The processes of technological innovation | SpringerLink. D.C. Heath & Company. 1990;298. Available from: https://books.google.com/books/about/The_Processes_of_Technological_Innovatio.html?id=EotRAAAAMAAJ
20. Vial G. Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems. 2019;28(2):118-144. doi:10.1016/J.JSIS.2019.01.003
21. Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. Management Information Systems Quarterly, 26(2), xiii–xxiii. https://doi.org/10.2307/4132319
22. Yu, J., Chiriko, A. Y., Kim, S. (Sam), Moon, H. G., Choi, H., & Han, H. (2025). ESG management of hotel brands: A management strategy for benefits and performance. International Journal of Hospitality Management, 125, 103998. https://doi.org/10.1016/J.IJHM.2024.103998
23. Zuhri MZ, Jaafar MN, Ab. Azis SS, Abdullah S, Vilessuzanne CC, Afrane E. A Likert–AHP Decision Model for Prioritising Hotel Business Takeover Strategies in Malaysia: Evidence from Kuala Lumpur. International Journal of Built Environment and Sustainability. 2026;13(3):335-342. doi:10.11113/ijbes.v13.n3.1739

How to Cite This Article
Zuhri MZ, Jaafar MN. Digital technology readiness for hotel business takeovers in Malaysia: a due diligence framework. Int J Multidiscip Res Growth Eval. 2026;7(6):112-118. doi:10.54660/.IJMRGE.2026.7.6.112-118.

Creative Commons (CC) License
This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms