Information System Audit Based on ISO/IEC 27001: A Case Study of a Culinary Small and Medium Enterprise

Mira Agustia[1*], Andini Syahputri[2] , Rizky Natasya[3], Neng Sri Wardhani[4]

[1,2,3,4]Department of Accounting, Universitas Pembangunan Panca Budi, Medan, Indonesia
E-mail : miraagustia74@gmail.com[1], andinisyahputri78@gmail.com[2], rizkynatasya71@gmail.com[3], nengsri_wardhani@dosen.pancabudi.ac.id[4]
E-mail Correspondece Author: miraagustia74@gmail.com

Abstract

Small and Medium Enterprises (SMEs) increasingly rely on information systems to support operational efficiency, customer management, and financial transactions. However, limited awareness and resources often cause SMEs to neglect information security governance, exposing them to data breaches and operational risks (ENISA, 2021). This study aims to evaluate the effectiveness of information security controls in a culinary SME using the ISO/IEC 27001 framework. A qualitative case study approach was employed, involving document analysis, interviews, and observation of information system practices within the organization (Yin, 2018). The audit results reveal several gaps in information security implementation, particularly in access control, risk assessment, and incident management. These findings indicate that although basic controls are in place, the SME has not yet aligned its practices with ISO/IEC 27001 requirements. This study contributes by providing a practical audit model for SMEs to improve information security governance in a cost-effective and structured manner (ISO, 2022).

Keywords : ISO/IEC 27001, Information System Audit, Information Security, SMEs, Case Study.

I. INTRODUCTION

The rapid digitalization of business processes has significantly transformed the operational landscape of Small and Medium Enterprises (SMEs), including those operating in the culinary sector (OECD, 2020). Information systems such as Point of Sale (POS), inventory management, and customer databases have become critical assets that support daily business activities and strategic decision-making (Laudon & Laudon, 2022).

Despite these benefits, SMEs often face substantial challenges in managing information security due to limited financial resources, lack of expertise, and low awareness of cybersecurity risks (Ahmad et al., 2021). As a result, SMEs are increasingly vulnerable to threats such as data leakage, unauthorized access, and system downtime, which may lead to financial losses and reputational damage (Verizon, 2023). Information system audits play a crucial role in evaluating the adequacy and effectiveness of security controls implemented within organizations (Hall, 2016). Through systematic assessment, audits help organizations identify weaknesses, ensure compliance with standards, and improve governance structures related to information security management (ISACA, 2019).

ISO/IEC 27001 is an internationally recognized standard that provides requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) (ISO, 2022). The standard is applicable to organizations of all sizes and sectors, making it particularly relevant for SMEs seeking structured yet flexible security frameworks (Humphreys, 2017).

Although numerous studies have discussed ISO/IEC 27001 implementation in large organizations, empirical research focusing on SMEs, especially in the culinary sector, remains limited (Tsohou et al., 2021). This research gap highlights the need for practical case studies that demonstrate how ISO/IEC 27001-based audits can be applied in SME contexts.

Therefore, this study aims to conduct an information system audit based on ISO/IEC 27001 in a culinary SME through a case study approach. The objectives of this study are to assess current security practices, identify gaps against ISO/IEC 27001 controls, and provide recommendations for improving information security governance in SMEs (Yin, 2018).

II. LITERATURE REVIEW

2.1 Information System Audit

An information system audit is a systematic process of collecting and evaluating evidence to determine whether an information system safeguards assets, maintains data integrity, and supports organizational objectives effectively (Hall, 2016). Audits are essential in ensuring that information systems operate securely and efficiently within established control frameworks (Romney & Steinbart, 2021).

In the context of SMEs, information system audits are often informal or ad hoc, leading to inconsistent control implementation and weak security posture (Ahmad et al., 2021). This condition emphasizes the importance of adopting standardized audit frameworks to enhance consistency and reliability in security assessments (ISACA, 2019).

2.2 ISO/IEC 27001 Framework

ISO/IEC 27001 specifies requirements for establishing an ISMS based on a risk management approach (ISO, 2022). The standard emphasizes the identification of information security risks, selection of appropriate controls, and continuous improvement through the Plan-Do-Check-Act (PDCA) cycle (Humphreys, 2017).

Annex A of ISO/IEC 27001 provides a set of reference controls covering organizational, people, physical, and technological aspects of information security (ISO, 2022). These controls serve as a comprehensive guideline for organizations to mitigate risks and protect information assets systematically (Calder & Watkins, 2018).

2.3 Information Security in SMEs

SMEs generally have lower maturity levels in information security management compared to large enterprises (ENISA, 2021). Factors such as limited budgets, lack of formal policies, and reliance on third-party IT services often hinder the implementation of comprehensive security controls (Tsohou et al., 2021).

However, previous studies indicate that adopting international standards like ISO/IEC 27001 can significantly improve security awareness and control effectiveness in SMEs, provided that the implementation is tailored to organizational context and capacity (Ahmad et al., 2021).

III. RESEARCH METHODOLOGY

This study employs a qualitative case study approach to gain an in-depth understanding of information security practices within a culinary SME (Yin, 2018). The case study method is suitable for exploring complex organizational phenomena in real-world contexts, particularly when boundaries between phenomenon and context are not clearly defined (Creswell, 2018).

The object of this study is a fictitious culinary SME operating multiple food outlets and utilizing information systems such as POS, inventory management software, and cloud-based accounting applications. The organization processes customer data, transaction records, and supplier information as part of its daily operations (Laudon & Laudon, 2022).

Data collection techniques include semi-structured interviews with management and staff, document analysis of existing policies, and direct observation of system usage and security practices (Creswell, 2018). These techniques enable data triangulation to enhance the validity of findings (Yin, 2018). The audit process follows ISO/IEC 27001 requirements, focusing on selected Annex A controls relevant to SME operations. Each control is assessed based on its existence, implementation level, and effectiveness in mitigating identified risks (ISO, 2022).

IV. RESULTS AND DISCUSSION

4.1 Overview of Current Information Security Practices

The audit findings indicate that the SME has implemented basic security measures, such as user authentication for POS systems and regular data backups. However, these practices are largely informal and undocumented, resulting in inconsistent application across business units (Hall, 2016).

The absence of formal information security policies reflects a common challenge among SMEs, where operational priorities often outweigh governance considerations (ENISA, 2021). This condition increases the likelihood of human errors and security incidents.

4.2 ISO/IEC 27001 Control Mapping

ISO27001 Control	Description	Current Practice	Gap
A.5 Information Security Policies	Establishment of policies	No formal policy	High
A.8 Asset Management	Asset identification	Partial inventory	Medium
A.9 Access Control	User access management	Basic login	Medium
A.12 Operations Security	Backup procedures	Regular backup	Low
A.16 Incident Management	Incident handling	No procedure	High

The mapping results show significant gaps in policy development and incident management controls, indicating misalignment with ISO/IEC 27001 requirements (ISO, 2022). These gaps may expose the organization to prolonged disruptions in the event of security incidents (Calder & Watkins, 2018).

4.3 Risk Analysis and Discussion

Based on the identified gaps, the highest risks relate to unauthorized access and delayed incident response. Without formal access control policies and incident management procedures, the SME may struggle to detect and respond to security breaches effectively (Verizon, 2023).

These findings align with previous studies highlighting that SMEs often underestimate information security risks until incidents occur (Ahmad et al., 2021). Implementing ISO/IEC 27001 controls incrementally could help SMEs enhance security maturity while considering resource constraints (Humphreys, 2017).

V. CONCLUSION

This study demonstrates that an ISO/IEC 27001-based information system audit provides a structured and practical approach for assessing information security in culinary SMEs. The findings reveal that while basic technical controls exist, significant gaps remain in governance, documentation, and incident management (ISO, 2022).

The study contributes to the literature by offering an applied case study that illustrates how international standards can be adapted to SME contexts. Practically, the results serve as guidance for SME owners and policymakers in improving information security governance (OECD, 2020).

However, this study is limited to a single fictitious case, which may restrict generalizability. Future research could involve multiple real-world SMEs and integrate quantitative risk assessment methods to strengthen empirical evidence (Yin, 2018).

VI. RECOMMENDATIONS

A. Recommendations for SMEs

Based on the audit results, culinary SMEs are strongly encouraged to establish a formal Information Security Management System (ISMS) aligned with ISO/IEC 27001 requirements. Management commitment is essential to ensure that information security policies are formally documented, approved, and consistently implemented across daily operations (ISO, 2022). This step provides a structured foundation for managing information security risks in a sustainable manner (Humphreys, 2017).

Culinary SMEs should prioritize the identification and classification of information assets, including POS systems, customer data, supplier records, and financial information. Maintaining a simple asset register and assigning asset ownership can significantly improve accountability and control effectiveness without imposing excessive administrative burden (Calder & Watkins, 2018). Proper asset management enables SMEs to focus security efforts on high-impact assets (ENISA, 2021).

Access control practices should be strengthened by applying role-based access control (RBAC) to information systems used in daily operations. User access rights should correspond to job responsibilities, and access reviews should be conducted periodically, particularly in environments with high staff turnover such as the culinary sector (Hall, 2016). These measures reduce the risk of unauthorized access and data misuse (ISO, 2022).

Culinary SMEs are also advised to formalize incident management procedures by developing simple guidelines for incident identification, reporting, and response. Even basic incident response documentation can help organizations respond more effectively to security incidents and minimize operational disruptions (Verizon, 2023). Establishing an incident log supports continuous improvement and accountability (Ahmad et al., 2021). Furthermore, regular information security awareness training should be provided to employees to mitigate human-related risks. Training programs focusing on password hygiene, phishing awareness, and secure system usage have been shown to be cost-effective controls for SMEs with limited resources (ENISA, 2021). Improving employee awareness directly contributes to strengthening the overall security posture of the organization (ISO, 2022).

B. Recommendations for Future Researchers

Future researchers are encouraged to extend this study by conducting empirical research involving multiple real-world culinary SMEs to enhance the generalizability of findings. Comparative studies across different SME sectors may provide deeper insights into sector-specific information security challenges and control effectiveness (Yin, 2018). Subsequent research may also integrate quantitative risk assessment methods, such as risk scoring or maturity models, to complement qualitative audit findings. Combining qualitative and quantitative approaches could provide a more comprehensive evaluation of information security implementation in SMEs (Creswell, 2018).

Additionally, future studies could explore the integration of ISO/IEC 27001 with other governance or audit frameworks, such as COBIT or NIST, to assess their combined effectiveness in improving information security governance in SMEs. This approach may offer practical guidance for organizations seeking more holistic security management frameworks (ISACA, 2019).

Finally, researchers are encouraged to examine the long-term impact of ISO/IEC 27001 implementation on SME performance, resilience, and competitiveness. Longitudinal studies could provide valuable evidence on how sustained information security practices contribute to business continuity and organizational growth over time (OECD, 2020).

VII. REFERENCES

Ahmad, A., Bosua, R., & Scheepers, R. (2021). Protecting organizational information assets: A risk-based approach to information security management. *Information Management &*

Computer Security, 29(1), 1–17. https://doi.org/10.1108/IMCS-06-2020-0184

Calder, A., & Watkins, S. (2018). *IT Governance: An International Guide to Data Security and ISO/IEC 27001* (6th ed.). Kogan Page.

Creswell, J. W. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). Sage Publications.

ENISA. (2021). *Cybersecurity for Small and Medium-Sized Enterprises*. European Union Agency for Cybersecurity.

Hall, J. A. (2016). *Information Technology Auditing and Assurance* (4th ed.). Cengage Learning.

Humphreys, E. (2017). *Implementing the ISO/IEC 27001 Information Security Management System* (3rd ed.). Artech House.

ISACA. (2019). *Information Systems Auditing: Tools and Techniques*. ISACA Press.

ISO. (2022). *ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*. International Organization for Standardization.

ISO. (2022). *ISO/IEC 27002:2022 — Information Security Controls*. International Organization for Standardization.

Laudon, K. C., & Laudon, J. P. (2022). *Management Information Systems: Managing the Digital Firm* (17th ed.). Pearson Education.

OECD. (2020). *SME and Entrepreneurship Policy in the Digital Era*. OECD Publishing. https://doi.org/10.1787/3c8b5171-en

Romney, M. B., & Steinbart, P. J. (2021). *Accounting Information Systems* (15th ed.). Pearson Education.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees’ adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Tsohou, A., Karyda, M., & Kiountouzis, E. (2021). Analyzing information security management in small and medium enterprises: A socio-technical perspective. *Computers & Security*, 105, 102–118. https://doi.org/10.1016/j.cose.2021.102118

Verizon. (2023). *Data Breach Investigations Report*. Verizon Enterprise Solutions.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning.

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). Sage Publications.