Check for updates

Jurnal Siasat Bisnis Vol.30 No. 2, 2026, 156-171

Jurnal SIASAT BISNIS

Journal homepage: https://www.journal.uii.ac.id/jsb

A vulnerability management model for enhancing security governance capability in SMEs

Anita Wijayanti[1*], Massila Kamalrudin[2], Kartika Hendra Titisari[3], Werner R Murhadi[4]

[1,3]Universitas Islam Batik Surakarta, Surakarta, Indonesia

[2]Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia

[4]Universitas Surabaya, Surabaya, Indonesia

[*]Correspondents e-mail: itax_solo@yahoo.com

Article Info

Article history:
Received : 2025-10-28
Accepted : 2026-06-30
Published: 2026-07-22

JEL Classification Code:
D80, M41, M48

Author's email:
massila@utem.edu.my
kartikatitisari@gmail.com
werner@ubaya.ac.id

DOI: 10.20885/jsb.vol30.iss2.art2

Abstract

Purpose – This study aims to develop a vulnerability management model to enhance security capability in small and medium-sized enterprises (SMEs), particularly in safeguarding accounting data under resource constraints

Design/Methodology/Approach – This study employs a qualitative multi-case research design involving six SMEs in Surakarta, Indonesia. Data were collected through in-depth interviews, direct observations, and document analysis. Using inductive comparative logic and cross-case thematic analysis, the study identifies recurring governance patterns and develops a context-sensitive vulnerability management model grounded in empirical evidence across varying levels of resource constraints.

Findings – The findings reveal that vulnerability management effectiveness in SMEs is shaped by the integration of governance structures, managerial coordination, and organizational learning rather than by technological capability alone. The study identifies three distinct governance configurations across SMEs under varying levels of resource constraints: reactive centralization, vendor-dependent compliance, and institutionalized adaptive governance. The proposed model consists of four interconnected components: identification and detection, evaluation and prioritization, managerial decision integration, and HR awareness and continuous learning. These components operate through a continuous feedback mechanism that strengthens adaptive security governance and organizational resilience.

Research Limitations and Implications – This study is limited to six SME cases in Surakarta, Indonesia, which may restrict broader generalizability across industries and regions. Future research may apply quantitative or mixed-method approaches to validate and extend the proposed model across different organizational and institutional contexts.

Practical implications – The study provides a practical and cost-efficient framework for SMEs to strengthen accounting data security through structured vulnerability management, risk-based prioritization, internal governance coordination, and continuous security awareness practices.

Originality/Value – This study positions vulnerability management as a governance-oriented and learning-based organizational capability shaped by resource conditions, managerial integration, and adaptive organizational practices. The proposed model offers a context-sensitive approach for strengthening sustainable accounting data security governance in SMEs.

Keywords: Vulnerability Management; Accounting Information Security; SME Governance; Resource Constraints; Cybersecurity Capability

P ISSN 0853-7666 | E ISSN 2528-7001

Copyright © 2026 Authors. This is an open-access article distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (http://creativecommons.org/licences/by-sa/4.0/)

Introduction

In recent years, the rapid shift toward a digital economy has elevated accounting data into a critical organizational asset, particularly for small and medium-sized enterprises (SMEs)(Schilirò, 2024; Wijayanti, 2018). The increasing adoption of digital accounting systems improves operational efficiency but simultaneously exposes SMEs to growing cybersecurity vulnerabilities, including ransomware attacks, unauthorized access, and financial data breaches (Adejumo & Ogburie, 2025; Chotia et al., 2025). Compared to large organizations with advanced cybersecurity infrastructure, SMEs commonly operate under significant resource constraints, including limited financial capacity, inadequate technical knowledge, and simplified technological infrastructure (Mazzano, 2025; Neri et al., 2022). These conditions limit their ability to systematically identify, assess, and manage vulnerabilities in accounting information systems (Jiang et al., 2025; Zlati et al., 2022).

Vulnerability management has been widely recognized as an important mechanism for identifying and mitigating cybersecurity risks (Bennouk & Aali, 2024; Zlati et al., 2022). However, existing studies predominantly emphasize technical detection and remediation processes while giving limited attention to how vulnerability assessment outcomes are integrated into managerial decision-making, governance structures, and organizational learning practices, particularly in SMEs operating under resource constraints (Adejumo & Ogburie, 2025; Roup & Effendy, 2025). In practice, many SMEs still rely on reactive security practices, informal coordination, and vendor-dependent arrangements that weaken internal governance capability and limit sustainable cybersecurity management (Isa et al., 2024; Mazzano, 2025).

Motivated by these gaps, this study develops a vulnerability management model that enhances security capability in SMEs, particularly in safeguarding accounting data. Using a qualitative multi-case approach involving six SMEs in Surakarta, Indonesia, the study explores how vulnerability identification, evaluation, managerial integration, and organizational learning interact under varying levels of resource constraints. Through cross-case comparison, the study explains how governance configurations shape vulnerability management practices and organizational security capability.

Theoretically, this study contributes to the vulnerability management literature by adopting a governance-oriented perspective that emphasizes managerial integration, organizational learning, and resource conditions as central determinants of cybersecurity capability in SMEs. Practically, the proposed model offers a context-sensitive and cost-efficient framework that enables SMEs to strengthen accounting data security through structured vulnerability management, governance coordination, and continuous learning mechanisms.

Literature Review

Vulnerability Management as a Governance Process

Vulnerability management is widely recognized as an important mechanism for identifying, assessing, and focusing on cybersecurity risks within organizational systems (Bennouk & Aali, 2024). Beyond technical detection, recent studies increasingly conceptualize vulnerability management as a continuous governance process integrating vulnerability assessment, risk evaluation, prioritization, and managerial decision-making (Giudiece, 2024; Jiang et al., 2025). Effective vulnerability management depends on detection capabilities and on the organization's ability to translate technical findings into coordinated governance practices and structured security responses (Shimizu & Hashimoto, 2025).

In SMEs, vulnerability management is strongly influenced by resource limitations, including financial constraints, limited technical knowledge, and simplified technological infrastructure (Isa et al., 2024; Mazzano, 2025). These conditions often lead SMEs to adopt reactive security practices, informal coordination, and vendor-dependent arrangements that weaken internal governance capability (Neri et al., 2022). Vulnerability management in SMEs should be understood not merely as a technical activity, but as a governance-driven organizational capability shaped by resource conditions and managerial integration.

Vulnerability Management in Accounting Information Systems

Within accounting information systems (AIS), vulnerability management plays a critical role in protecting sensitive financial data and supporting organizational continuity. Technical tools such as OpenVAS, OWASP ZAP, and NMAP help organizations to identify system weaknesses, access control gaps, and network vulnerabilities. However, prior studies emphasize that effective vulnerability management in AIS extends beyond technical scanning activities and includes risk evaluation, mitigation prioritization, policy enforcement, and continuous tracking (Roup & Effendy, 2025; Zlati et al., 2022).

Recent literature further highlights that vulnerability management contributes to system security and to financial stability, regulatory compliance, and stakeholder trust (Morshed, 2025). Nevertheless, existing studies remain largely tool-oriented and compliance-focused, with limited attention given to how vulnerability assessment outcomes are integrated into managerial decision-making, organizational learning, and governance processes within SMEs operating under resource constraints.

Resource Constraints and Governance Capability in SMEs

From a contingency perspective, the effectiveness of vulnerability management depends on the alignment between governance structures and organizational resource capacity (Shimizu & Hashimoto, 2025). SMEs commonly rely on simplified and semi-structured security practices due to limited financial resources, managerial resources, and technical capability (Isa et al., 2024). Vulnerability assessment outcomes are often interpreted through operational priorities and cost–benefit considerations rather than through formalized governance systems (Waweru et al., 2025).

From a dynamic capability perspective, vulnerability management can be viewed as an organizational capability involving detection, evaluation, and adaptive response processes (Jiang et al., 2025). However, the effectiveness of these processes is shaped by resource conditions that influence the organization's ability to identify risks, focus on responses, and institutionalize organizational learning. Building on past studies (Bennouk & Aali, 2024; Jiang et al., 2025; Mazzano, 2025; Shimizu & Hashimoto, 2025), this study develops a governance-oriented vulnerability management model emphasizing the interaction between detection, evaluation, managerial integration, and organizational learning in strengthening accounting data security capability among SMEs.

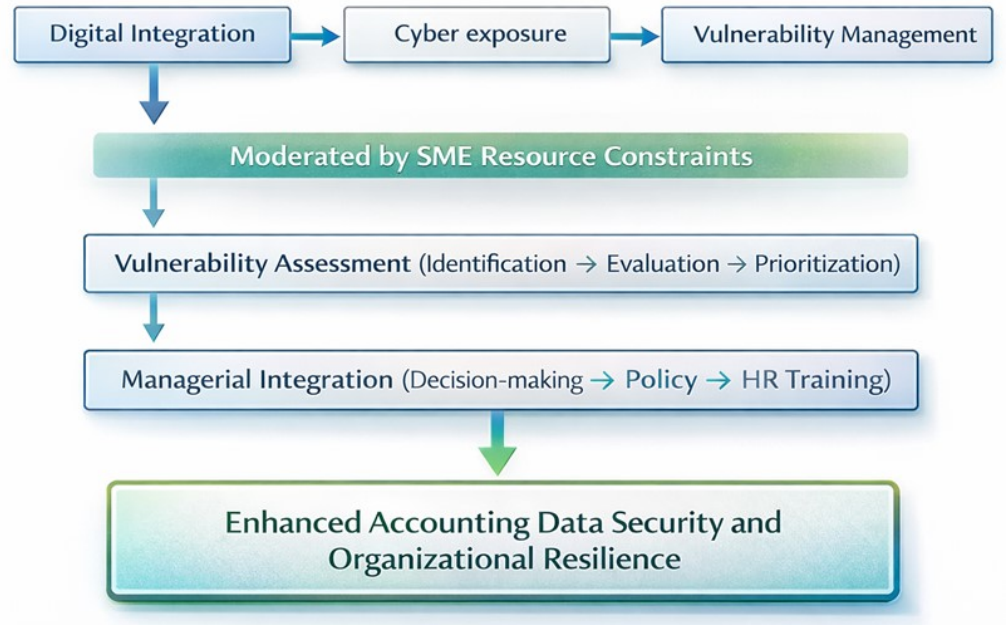

Figure 1. Conceptual Structure of Vulnerability Management SMEs
(Bennouk & Aali, 2024; Jiang et al., 2025; Mazzano, 2025; Shimizu & Hashimoto, 2025; Waweru et al., 2025)

Research Methods

This study adopts a multi-case qualitative design to examine how vulnerability management practices are integrated into governance processes in SMEs and to develop a context-sensitive model of security capability under resource constraints. The study specifically focuses on how vulnerability assessment processes are translated into managerial decision-making, organizational routines, and security governance practices across different levels of resource capacity. The research follows an inductive comparative logic, whereby patterns and mechanisms emerging across cases are synthesized into a coherent analytical framework (Eisenhardt et al., 2007; Yin, 2007). Positioned within a qualitative comparative tradition, the study contributes by refining models for resource-constrained SMEs, rather than by generating theory or testing deductive models (Thomann & Maggetti, 2020; Yin, 2011). Drawing on established vulnerability management, contingency, and dynamic capability perspectives, it extends prior conceptualizations by incorporating resource constraints as a central structural condition shaping the enactment of vulnerability management in SMEs. Through cross-case comparison, the study develops a context-conditioned refinement that explains how variations in organizational capacity generate distinct governance configurations in accounting data security management (Eisenhardt & Bourgeois, 1988). The study involves six SME cases in Surakarta, Indonesia, each employing fewer than 100 employees and having implemented a vulnerability management process to identify potential vulnerabilities in their accounting data systems. The choice of these six SMEs was preceded by an initial screening phase of 35 SMEs that met the basic inclusion criteria, specifically, enterprises with fewer than 100 employees that had adopted digital accounting systems supported by vulnerability assessment mechanisms.

The choice of the six cases was designed under the replication logic articulated by Eisenhardt (2007), thus strengthening theoretical inference rather than merely capturing empirical variation. The research design integrates both literal replication and theoretical replication to enhance cross-case analytical leverage. Two cases were purposively selected within each resource-constraint category (high, moderate, and low) to enable literal replication, letting the study examine whether similar vulnerability management mechanisms recur under comparable structural conditions. Comparisons across the three categories were structured as theoretical replication, grounded in the a priori assumption that variations in organizational resource capacity would systematically activate distinct governance configurations. Specifically, before data analysis, we expected that SMEs operating under high resource constraints would show reactive and owner-centered vulnerability practices; moderately constrained SMEs would develop more formal yet vendor-dependent arrangements; and low-constraint SMEs would institutionalize governance routines and learning-based adaptation (Eisenhardt et al., 2007; Yin, 2011). For example, SMEs that relied on reactive practices gradually developed more structured tracking and response mechanisms after experiencing security incidents. These expectations guided the replication logic and structured the cross-case comparison (Eisenhardt et al., 2007; Hollweck, 2016; Ridder, 2017).

Inter-case differences are not interpreted as simple gradations of maturity, but as manifestations of qualitatively distinct causal mechanisms in the integration of vulnerability detection, risk evaluation, managerial decision-making, and organizational learning (Yin, 2011). Within this framework, resource constraints are conceptualized as structural conditions that moderate the enactment of vulnerability management capabilities (Eisenhardt et al., 2007; Yin, 2011). This design enables the study to explain how variations in organizational capacity produce differentiated configurations of accounting data security governance, thereby reinforcing the theoretical contribution of the research by positioning vulnerability management as a context-conditioned organizational capability shaped by underlying resource structures (Eisenhardt et al., 2007; Ridder, 2017).

Subsequently, each SME was evaluated using a resource constraint scoring rubric that comprises four key dimensions: (1) the proportion of budget allocated to information technology and security, (2) the capacity and competence of IT-related human resources, (3) the quality of infrastructure and security tools, and (4) the existence of formal security policies and employee training programs. The total scores across these dimensions were used to classify SMEs into three

resource-constraint categories: high, moderate, and low. The Resource Constraint Scoring Rubric for SME Case Classification is presented in Table 1. Based on this classification, six SMEs representing varying levels of resource capacity were purposively selected as case samples for the comparative multi-case study (Bouncken et al., 2025).

Table 1. Resource Constraint Scoring Rubric for SME Case Classification

Dimension/Score	0 (High Capacity)	1 (Moderate Capacity)	2 (Low Capacity)	3 (Very Low Capacity)
IT Budget	>5%	2–5%	1–2%	<1%
IT HR	≥3 certified staff	1–2 IT staff	Non-IT handling IT	None
Infrastructure	ERP/core banking	Cloud AIS	Basic software antivirus	Manual/Excel
Policies & Training	Formal + regular	Limited policies	Ad-hoc training	None

The 0–3 scoring thresholds were established using an ordinal categorization approach commonly applied in multi-case research to enable systematic comparison across organizations (Bouncken et al., 2025). Each threshold came from clearly defined operational indicators, such as the percentage of the IT budget, the number and competence of IT staff, the digital infrastructure, and formal security policies, thus reducing subjective judgment. Accuracy was further strengthened through triangulation of interviews, observations, and document analysis (Bouncken et al., 2025; Jiang et al., 2025). To improve reliability, two independent raters conducted the assessments separately, followed by calibration sessions and inter-researcher convergence discussions to reconcile any differences (Bouncken et al., 2025; Rusu & Mantulescu, 2025).

The results of the resource constraint scoring analysis identified six SMEs that met the selection criteria and were used as case samples in the multiple-case study. These SMEs are presented in Table 2.

Table 2. Profile of the Selected SME Cases

Case	Type of Business/Industry	Number of Employees	Level of Resource Constraints
A	Culinary (Ready-to-eat food)	25	High
B	Retail clothing	30	High
C	Digital printing	45	Moderate
D	Rural Bank	80	Moderate
E	Batik manufacturing	75	Low
F	Food distribution	90	Low

The systematic selection process ensured that each case represented the diversity of resource conditions and contextual realities among SMEs in Surakarta. The study aims to develop a vulnerability management model that is contextual, adaptive, and almost relevant for SMEs in strengthening the governance of accounting data security.

Subsequently, data collection was conducted through three primary qualitative methods: in-depth interviews, direct observation, and document analysis. The respondents in this study consisted of key managerial and operational personnel from the six SMEs selected as research cases in Surakarta. Each case involved three to four informants representing different organizational roles directly related to digital accounting data management, system operations, and cybersecurity governance.

Informants were purposively selected based on their direct involvement in the planning, implementation, or supervision of digital accounting systems and data security processes within their respective organizations. 22 informants participated in the study, representing managerial, financial, technical, and administrative roles. The distribution of informants across the six cases is presented in Table 3.

The collected data were analyzed using a two-layered thematic analysis, consisting of: 1) Within-case analysis, which tried to identify and understand specific patterns within each SME regarding how vulnerabilities in accounting systems were detected, assessed, and managed; 2)

Cross-case comparative analysis, conducted to compare the similarities and differences across SMEs based on their levels of resource constraints high, moderate, and low; and Conditional Coding, employed to interpret how resource constraints moderated the relationships between digital integration, cyber exposure, and the effectiveness of vulnerability management.

Table 3. Distribution of Respondents across SME Cases

Case	Number of Respondents	Respondent Positions / Roles
A	3	1. Owner/Director, 2. Finance Staff, 3.Cashier/Administrator
B	3	1. Owner, 2. Accounting Officer, 3. IT Support (outsourced)
C	4	1. Owner, 2. Finance Manager, 3. IT Technician, 4. HR Officer
D	4	1. Head of IT Division, 2. Internal Auditor, 3. Finance Manager, 4. HR/Compliance Officer
E	4	1. Owner, 2. Finance Head, 3. IT Staff. 4. Production Manager
F	4	1. Director, 2. Accounting Manager, 3. IT System Administrator, 4. HR Officer

The coding procedure was conducted in sequential stages. First, open coding was performed within each case to identify initial concepts emerging from the interview data. Second, cross-case axial coding refined and group categories based on emerging causal relationships. Finally, conditional coding was applied to construct the theoretical mechanisms linking empirical findings to the proposed model. Codes were developed through iterative comparison across cases, refined through researcher discussions, and confirmed using member checking and a coding audit trail.

To ensure analytical consistency, two independent coders conducted the initial coding separately. Minor discrepancies in code labeling and category grouping were resolved through convergence discussions and re-examination of transcripts until conceptual agreement was achieved. This intersubjective validation process, supported by a coding audit trail and member checking, strengthened the credibility and dependability of the findings. Thematic saturation was achieved when the final two cases did not generate new first-order codes or thematic categories but instead reinforced previously found analytical patterns. Given the replication logic underlying case selection, the stabilization of findings across resource-constraint categories indicates that the data were sufficiently rich to support model refinement.

The model-building process was conducted systematically through four sequential stages: (1) Theme Identification, derived from thematic coding and cross-case analysis to identify key categories and recurring patterns; (2) Thematic Mapping, using a pattern-matching technique to establish cause-and-effect relationships among emerging themes; (3) Conceptual Synthesis, in which analytical patterns were integrated into a multi-layered framework illustrating the process of input, process, output, and feedback loop; and 4) Model Verification, conducted through member checking to make sure the model accurately reflected empirical realities and expert review, involving cybersecurity and SME management experts who assessed the model's relevance, feasibility, and theoretical consistency.

The multi-layered analytical approach used in this study provides a strong methodological foundation for finding recurring patterns, contextual dynamics, and causal relationships across the six SME cases analyzed, supporting the proposed model. Although the study involves six SME cases, saturation was achieved through purposeful sampling and replication logic. The final two cases did not generate new first-order codes or thematic categories; instead, they reinforced existing analytical patterns identified in earlier cases. This pattern stabilization indicates thematic saturation within the defined research scope. The use of literal and theoretical replication strengthens analytical generalization, as cases were selected not for statistical representativeness but for configurational contrast across resource levels. In multi-case qualitative research aimed at model refinement, depth of cross-case replication is focused on over numerical breadth, thus supporting the adequacy of six strategically selected cases.

Results and Discussion

Governance Configuration and Resource Alignment in SME Vulnerability Management

These variations also reflect differences in SMEs' capacity to adapt to disruptions and develop resilience over time, as shown by how firms respond to security incidents, adjust internal processes, and strengthen their governance practices. The findings indicate that differences in vulnerability management practices across SMEs are associated with technological capacity and with variations in organizational security capability. This capability is reflected in how SMEs integrate vulnerability detection, managerial coordination, risk evaluation, and organizational learning into their governance practices.

In highly resource-constrained firms (Cases A–B), digital integration was primarily efficiency-driven and lacked formalized security controls. The owner of Case A explained, "We just use the main account for all payments, so there's no need for multiple logins." (Owner, Case A). Similarly, the accounting staff in Case B admitted, *"Customer transaction data is automatically transferred to my personal laptop, it's faster that way, though we've never encrypted it."* (Accounting Staff, Case B). These findings illustrate a governance gap in vulnerability management, where technical activities are disconnected from formal decision-making structures, documented policies, and coordinated security responsibilities.

The evidence suggests that operational convenience is focused on over security governance, resulting in weak segregation of duties, limited access control, and the absence of basic data protection mechanisms such as encryption. The use of shared accounts reduces accountability and increases the risk of unauthorized access, while storing financial data on unsecured personal devices heightens exposure to potential data breaches and data integrity failures. Under severe resource constraints, vulnerability management practices therefore remain informal and reactive rather than institutionally embedded within organizational governance structures. This condition indicates that limited resource capacity constrains technological implementation and weakens the integration of security practices into managerial coordination and organizational control mechanisms.

The use of a single account for all transactions, data transfers to personal devices without encryption, and the absence of multi-factor authentication, routine backups, and automatic system updates indicate a weak control architecture. At a moderate level (Cases C–D), integration was more structured through vulnerability scanning services and banking system connectivity; however, access rights management and security audits remained vendor-dependent, with limited internal follow-up. This condition suggests that, while these firms have adopted more formalized practices, their internal security capability remains underdeveloped because improvements are primarily triggered by external actors rather than internally established governance mechanisms.

The IT staff of Case C noted, *"We subscribed to vulnerability scanning services, but the results haven't yet been followed up on."* (IT Staff, Case C). In Case D, the head of the IT division stated, *"We submit monthly reports to the Financial Services Authority via core banking, but we rely on vendors for security audits."* (Head of IT, Case D). Observations further revealed that vendors held administrator privileges without direct supervision, while system logs were kept for only 90 days. These findings indicate that, although SMEs at this level have adopted more formalized cybersecurity tools and procedures, their implementation remains incomplete and externally driven. The reliance on vendors not only limits internal control and tracking capacity but also constrains the organization's ability to independently detect, interpret, and respond to cybersecurity risks. This condition reflects a transitional governance structure, where cybersecurity practices are compliance-oriented rather than strategically embedded. Vulnerability management fails to evolve into an internally embedded organizational capability, thus limiting the development of sustainable security governance practices.

Firms with stronger capacity (Cases E–F) implemented role-based access control, early warning systems, automated backups, active firewalls, backup servers, and periodic security training within a formalized and documented governance framework. The company director stated, *"Whenever there's unusual activity, the system immediately sends alerts. We also conduct security training twice a*

year" (Director, Case E/F). This statement indicates that cybersecurity practices in these firms are technologically supported and systematically embedded within organizational routines. Real-time tracking systems and regular training programs reflects a proactive approach to risk management, in which potential threats are expected and discussed before escalating into major incidents.

For instance, some SMEs reported system disruptions that prompted immediate procedural adjustments and increased tracking activities. Following such disruptions, SMEs shifted from reactive and informal practices toward more structured tracking, formalized procedures, and stronger governance coordination. This configuration demonstrates a higher level of governance maturity, where vulnerability management is institutionalized and integrated across technical and human dimensions. These firms show stronger security capability, reflected in their ability to coordinate tracking processes, implement structured risk responses, and continuously strengthen organizational security practices.

These findings demonstrate that technological connectivity does not automatically strengthen organizational security capability. Under resource constraints, digital integration enhances speed and operational efficiency but simultaneously expands the risk surface when not supported by formal control structures and tracking mechanisms. This condition is reflected in statements such as, *"The system is faster, but we don't really control who can access the data."* (Owner, Case A), suggesting that efficiency is often focused on over security governance. In transitional settings, risk awareness begins to emerge, yet security practices remain compliance-oriented and externally dependent. As noted by one informant, *"We follow the vendor's audit requirements, but we don't conduct internal evaluations."* (IT Staff, Case C), suggesting that security practices are implemented primarily to satisfy external requirements rather than internal risk management priorities.

Digital integration contributes to stronger security capability only when aligned with governance structures, structured access controls, continuous tracking, and strengthened human capacity. This is clear in more advanced SMEs, where *"We routinely monitor system access and receive immediate alerts when suspicious activity occurs."* (IT Manager, Case E). Thus, the primary distinction across SMEs lies not in technological sophistication but in the degree of institutionalized digital risk governance.

A similar pattern appears in vulnerability assessment practices. In highly constrained SMEs, assessment activities are reactive and incident-based, lacking standardized procedures and formal risk documentation, reflecting a perception of cybersecurity as a technical disruption rather than a strategic governance issue. This is supported by statements such as, *"We usually only check the system when something goes wrong"* (Admin, Case A), suggesting the absence of systematic assessment routines. At the moderate level, procedures are formalized through annual audits and vendor reviews; however, mitigation priorities remain driven more by regulatory demands than by internal risk mapping or accounting data sensitivity. As expressed by another informant, "All system security matters still depend on external vendors." (Head of IT, Case D), highlighting continued reliance on external actors.

But firms with stronger governance conduct routine access tracking, automated alerts for suspicious activity, and periodic incident simulations supported by documented security records. One respondent explained, *"Every security incident is evaluated and used to improve our system going forward."* (Director, Case F), demonstrating structured evaluation and organizational learning mechanisms.

Analytically, these differences indicate that assessment effectiveness depends less on the availability of tools than on process internalization within the organization. In reactive configurations, vulnerability management remains fragmented and disconnected from strategic governance processes, thus limiting organizational learning. Transitional configurations reduce operational disorder through procedural formalization but remain constrained by vendor dependency. Sustainable security capability emerges when vulnerability assessment functions as an integrated organizational learning mechanism embedded within policy, training, tracking, and cross-functional decision-making. This is reflected in statements such as, *"We don't just fix problems; we make sure they don't happen again through training and evaluation."* (HR Officer, Case F), suggesting the transformation of security practices into continuous organizational learning processes. Managerial integration becomes the central explanatory mechanism, showing effective vulnerability

management in SMEs is shaped not by technology alone, but by the institutionalization of coherent and continuous governance structures.

Taken together, these within-case observations indicate systematic differences in how managerial integration evolves across varying levels of resource availability. Building on this pattern, the cross-case analysis identifies three governance configurations in SME vulnerability management practices across resource levels. Rather than reflecting a linear maturity progression, these patterns represent structurally differentiated mechanisms. To clarify these contrasts, Table 4 presents a structured comparison across analytical dimensions.

Table 4. Cross-Case Comparison of Vulnerability Management Across Resource Levels

Analytical Dimension	High Constraint SMEs (A–B)	Moderate Constraint SMEs (C–D)	Low Constraint SMEs (E–F)
Detection Logic	Reactive, incident-triggered	Periodic, vendor-initiated scanning	Continuous internal monitoring
Risk Evaluation	Informal, intuitive judgment	Compliance-driven, vendor-reported	Risk-scoring matrix, impact-based
Decision Integration	Owner-centered, undocumented	Budget-dependent, semi-formal	Institutionalized, committee-based
Governance Structure	Centralized and informal	Vendor-mediated and compliance-oriented	Integrated cross-department governance
Organizational Learning	Minimal or absent	Limited to IT personnel	Organization-wide training and simulation
Dominant Mechanism	Reactive Centralization	Vendor-Dependent Compliance	Institutionalized Adaptive Governance

The comparison reveals three contrasting governance mechanisms. SMEs under high resource constraints exhibit reactive and individually driven practices characterized by centralized decision-making and informal risk handling. This is reflected in statements such as, *"Most decisions depend on the owner, and we don't have formal security procedures."* (Owner, Case B), indicating the absence of structured governance mechanisms. Moderately constrained SMEs demonstrate compliance-oriented yet vendor-dependent arrangements, where formal procedures exist but remain externally mediated. As noted by one informant, *"We follow standard procedures, but most of the security process is handled by external vendors."* (IT Staff, Case C), suggesting limited internal control and reliance on external knowledge. SMEs with lower resource constraints develop strategic and integrated systems in which vulnerability management is institutionalized, cross-functional, and reinforced through continuous organizational learning. This is supported by statements such as, *"We have regular coordination across departments, and security is part of our routine management meetings."* (Manager, Case E), reflecting a higher level of governance integration and organizational learning.

Beyond a descriptive association, resource constraints in this study function as structural configuration variables that condition the enactment of vulnerability management practices. Drawing on contingency theory, the effectiveness of vulnerability management is not determined by a universal best practice model, but by alignment between governance structures and organizational resource profiles. In highly constrained SMEs, limited financial allocation and technical knowledge compress decision authority and reduce formalization, thus producing reactive and centralized governance mechanisms. This is reflected in statements such as, *"We don't have enough budget or staff to manage security properly, so most decisions are handled directly by the owner."* (Owner, Case A), showing how resource scarcity shapes centralized and informal decision-making.

Under moderate constraints, partial resource availability enables procedural formalization but simultaneously fosters dependency on external vendors, inhibiting internal capability development. As noted by one informant, *"We have some procedures in place, but we still depend heavily on vendors for implementation and follow-up."* (IT Staff, Case C), suggesting that formalization does not necessarily translate into internal capability. Relatively resource-sufficient SMEs can institutionalize detection routines, put risk-based evaluation systems into practice, and distribute governance responsibilities across functional units. This is supported by statements such as, *"We assign*

responsibilities across departments and regularly evaluate risks as part of our management process." (Manager, Case E), reflecting a more integrated governance structure. Viewed through a dynamic capability perspective, limited resources influence how SMEs identify risks, choose responses, and change their internal systems. When resources are limited, firms may find it difficult to accurately detect vulnerabilities, focus on risks effectively, or turn security insights into ongoing organizational learning and adaptation. Thus, resource constraints operate not merely as boundary conditions but as enabling and inhibiting mechanisms that reshape the governance architecture of vulnerability management. This configurational role explains why vulnerability management effectiveness differs structurally, rather than incrementally, across resource levels.

The effectiveness of vulnerability management among SMEs is influenced by four interrelated factors derived from the empirical findings:

1. Resource Capacity and Technical Infrastructure.
   Firms assigning higher IT budgets (>5% of operational costs) showed systematic vulnerability assessments and faster remediation cycles, while those assigning <1% showed delayed patching and weak backup hygiene. This is reflected in statements such as, *"We don't have enough budget to regularly update or secure our systems."* (Owner, Case A), suggesting that limited financial resources directly constrain the implementation of effective security practices.
2. Managerial Integration and Decision Structures.
   Managerial participation in security governance emerged as an important determinant. In low-capacity firms (Cases A and B), security decisions were undocumented and owner-dependent. As noted by one informant, *"All decisions depend on the owner, and we don't have formal security procedures."* (Admin, Case B). Cases E and F institutionalized cybersecurity within their management routines through regular risk review meetings and structured coordination across departments.
3. Digital Integration and Cyber Exposure.
   The extent of digital interconnectivity significantly influenced cyber exposure levels. SMEs with extensive integration but weak controls (Cases A and B) faced high risks of unauthorized access and data breaches. This is illustrated by statements such as, *"Our system is connected, but we don't really monitor access or control user activities."* (Finance Staff, Case A). Conversely, firms with managed integration (Cases E and F) achieved both operational efficiency and lower cyber vulnerability.
4. Organizational Learning and Human Capacity.
   SMEs with stronger governance structures emphasized continuous learning through training and simulations, enabling employees to respond more effectively to cyber risks. This is reflected in statements such as, *"We regularly conduct training so employees understand how to handle security issues."* (HR Officer, Case F). Firms with limited capacity showed minimal awareness and lacked structured learning mechanisms.

Taken together, these findings indicate that effective vulnerability management in SMEs depends not only on technological investment, but on integrating governance structures, managerial coordination, and organizational learning processes.

The results of integrating the two-layered thematic analysis with the model development stages are presented in Table 5. This table demonstrates how recurring empirical patterns derived from interview data and cross-case comparison are systematically translated into the parts of the proposed model.

To synthesize these insights, following the presentation of within-case and cross-case findings, this section clarifies how each empirical theme informs the parts of the proposed model. Themes related to technological constraints, informal digital integration, and limited HR capacity shape the Identification and Detection stage. Reactive assessments, vendor dependency, and the absence of security policies underpin the Evaluation and Prioritization stage. Owner-driven decision-making, emerging risk meetings, and initial policy development guide the Managerial Decision Integration stage. Finally, cybersecurity training, incident simulations, and post-training evaluations are the Security Awareness and Organizational Learning part.

Table 5. Themes, Indicators, and Model Stages of the Vulnerability Model for SMEs

Theme	Key Indicators	Model Stage
Resource & Security Constraints	Minimal IT budget; no security tools or backups	Identification & Detection
Weak Digital Integration	No MFA; customer data stored on personal devices	Identification & Detection
Limited Technical HR	Non-IT staff manage systems; no audit/update skills	Identification → Evaluation
Reactive Vulnerability Checks	Checks only after failures; no SOP/policies	Evaluation & Prioritization
Vendor Dependency	External vendors control audits and admin access	Evaluation → Managerial Decision
Absence of Security Policies	No written rules; decisions rely on the owner's intuition	Managerial Integration
Risk Meetings & Coordination	Regular risk discussions across departments	Managerial Integration
Training & Organizational Learning	Regular training, simulations, and evaluations	HR Awareness & Continuous Learning

Collectively, these thematic relationships indicate that vulnerability management effectiveness in SMEs depends on integrating technical detection, managerial coordination, and organizational learning into coherent security governance practices.

These mappings come from recurring empirical patterns across cases. For example, themes such as reactive assessment and vendor dependency consistently emerged from informants' accounts, suggesting structural limitations in governance practices. This mapping demonstrates how the model's theoretical mechanisms directly come from empirical observations across the six SME cases. Linkages between the empirical themes and the model parts are presented in Table 6.

Table 6. Linkages Between Empirical Themes and Model Components

Empirical Theme	Model Component Influenced	Direction of Influence
Limited technological resources	Identification & Detection	Weakens early detection capability
Informal digital integration	Identification & Detection	Increases exposure to risks and vulnerabilities
Low technical HR competence	Identification & Evaluation	Reduces accuracy in identifying and focusing on risks
Reactive/undocumented assessments	Evaluation & Prioritization	Limits risk-based decision-making
Vendor dependency	Evaluation → Decision Integration	Decreases internal control and independent analysis
Absence of formal security policies	Decision Integration	Leads to inconsistent, ad hoc decisions
Cross-division risk meetings	Decision Integration	Strengthens coordination and governance
Security training and simulations	Continuous Learning	Enhances organizational adaptation and continuous improvement

The model illustrates that vulnerability management effectiveness in SMEs emerges from the interaction between technological conditions, governance structures, managerial integration, and organizational learning processes.

The Vulnerability Management Model for Resource-Constrained SMEs

Under disruption conditions such as system failures, cyberattacks, or data breaches, SMEs are required to respond rapidly and adjust their internal governance and security practices. The

proposed Vulnerability Management Model for SMEs represents the synthesized outcome of the thematic integration process derived from cross-case empirical findings. Rather than being based on abstract assumptions, the model reflects recurring governance patterns seen across SMEs operating under varying levels of resource constraints.

The model demonstrates the dynamic relationship between digital integration, resource constraints, and security governance capability, outlining how managerial, technical, and procedural dimensions interact to strengthen vulnerability management practices among SMEs. This relationship is reflected in statements such as, *"We don't just fix problems, but we also adjust our procedures and train staff so similar issues don't happen again."* (Manager, Case E), indicating that effective security practices are strengthened through continuous organizational learning, procedural improvement, and managerial coordination rather than through technology alone.

While the proposed model comes from cross-case empirical findings, its contribution lies in theoretical refinement and in its practical applicability within resource-constrained SME contexts. The model emphasizes continuous governance improvement, in which SMEs adjust their security practices in response to emerging risks, operational constraints, and evolving organizational needs. To clarify its operational relevance and context, the next section shows how the model can be made step by step in a low-capacity SME environment.

The proposed Vulnerability Management Model for SMEs is designed to help resource-constrained SMEs implement practical and sustainable vulnerability management practices without relying on high-cost technologies or specialized technical expertise. Rather than representing a linear technical procedure, the model functions as an integrated governance framework in which managerial coordination, risk evaluation, organizational learning, and security practices interact continuously. Conceptually, the model has four interrelated parts connected through a continuous improvement feedback mechanism that supports ongoing governance refinement and security capability development. These parts are prescriptive and come from recurring practices and cross-case empirical patterns seen across SMEs.

The model should not be interpreted as a linear technical procedure, but as an integrated governance framework in which vulnerability management practices are continuously shaped by managerial coordination, organizational learning, and resource conditions.

1. Identification and detection.
   The first stage focuses on identifying and detecting system vulnerabilities using open-source tools and internal manual verification. SMEs are encouraged to utilize tools such as OpenVAS or OWASP ZAP to scan their digital accounting systems and internal networks regularly. This reflects practices observed in several SMEs, where *"we use simple tools to check our system regularly because we cannot afford expensive security solutions"* (IT Staff, Case C), indicating how resource constraints shape practical detection strategies.
2. Evaluation and prioritization.
   The second stage emphasizes risk-based vulnerability evaluation, focusing on business impact over technical complexity. The model introduces a simple risk scoring matrix to classify findings based on their financial and operational implications. This approach aligns with SMEs' need to balance risk mitigation with limited resources, making sure decision-making remains practical and context-sensitive.
3. Managerial decision and policy integration.
   The third stage represents the central governance part of the model, where vulnerability evaluation results are translated into organizational decisions, security policies, and operational procedures. This stage emphasizes managerial coordination, risk communication, and integrating cybersecurity practices into routine organizational governance. SMEs at this stage begin to formalize security responsibilities, establish internal coordination mechanisms, and align vulnerability management activities with operational priorities and resource conditions. As reflected by one respondent, *"We discuss risks regularly and decide together what needs to be prioritized"* (Manager, Case E), highlighting the importance of managerial involvement in strengthening governance coordination and institutionalizing security practices within SMEs.

4. HR Awareness and Continuous Learning.
   The fourth stage centers on the human dimension, promoting security awareness and competency through recurring training and simulated cyber-incident exercises. This stage fosters a security-oriented organizational culture, making sure employees participate in safeguarding accounting data and supporting organizational security practices. Such practices reflect a transition from reactive security responses toward continuous organizational learning and security awareness within SMEs.
5. Continuous Improvement Feedback Mechanism.
   These four parts are interconnected through a continuous improvement feedback mechanism in which audit findings, cyber incidents, and operational disruptions contribute to the refinement of subsequent governance and security practices. Disruptions such as cyber incidents, system failures, or audit findings trigger processes of evaluation, response, and procedural change, enabling SMEs to strengthen managerial coordination and improve organizational preparedness. This mechanism lets vulnerability management practices remain context-sensitive and operationally feasible under resource constraints. As noted by one informant, *"Every issue becomes a lesson for us to improve our system and training"* (HR Officer, Case F), illustrating how continuous learning strengthens organizational security capability and governance improvement.

In this model, security capability refers to SMEs' ability to identify vulnerabilities, coordinate risk responses, strengthen governance practices, and continuously improve organizational preparedness under resource constraints.

Discussion

The findings suggest that cybersecurity effectiveness in SMEs depends less on technological sophistication and more on how resources are organized and governed within the firm. This follows the empirical evidence, where SMEs with limited technological capacity still managed risks through structured governance practices. For example, one informant noted, *"We may not have advanced systems, but we manage risks through regular coordination and monitoring."* (Manager, Case E), indicating that governance mechanisms can compensate for technological limitations.

While the TOE framework perspective emphasizes the interaction between technological and organizational elements (Nurwanah, 2024), and the Cyber ESP Framework highlights socio-technical balance (Mazzano, 2025), the present findings indicate that under resource constraints, this interaction becomes asymmetrical. When technological capacity is limited, governance structure and managerial integration function as compensatory mechanisms that translate constrained resources into coordinated control. Thus, security capability in SMEs is strengthened not primarily through technological optimization, but through governance alignment and the ability to coordinate practices under resource limitations.

This study further extends prior vulnerability research (Bennouk & Aali, 2024; Jiang et al., 2025; Mazzano, 2025; Shimizu & Hashimoto, 2025) by embedding vulnerability management within digital accounting and financial system integration. Empirical findings show that accounting data sensitivity shapes how SMEs prioritize risks and institutionalize security practices. As one respondent explained, *"We focus more on protecting financial data because it directly affects our business operations."* (Finance Manager, Case D), highlighting how context-specific priorities influence vulnerability management practices. Differences in vulnerability management effectiveness across SMEs reflect structurally distinct governance architectures rather than incremental capability gaps.

Moreover, the continuous improvement feedback mechanism identified in this study operates as a recursive governance process that institutionalizes organizational learning. This is reflected in practices where SMEs continuously adjust procedures based on past incidents, as noted by an informant: *"Every issue becomes a lesson for improving our system and training."* (HR Officer, Case F). In contrast to the Design Science Research-based framework (Mazzano, 2025), which emphasizes semi-automated asset–risk integration, and the Vulnerability Management Chaining Model (Mazzano, 2025; Shimizu & Hashimoto, 2025), which focuses on algorithmic detection

efficiency, the present model demonstrates that sustainable security governance capability depends on cross-functional decision institutionalization and human resource engagement. That means vulnerability management in SMEs should be conceptualized as a context-sensitive governance capability embedded within accounting control systems, where organizational learning mediates the transformation of technical findings into sustainable security governance practices.

Theoretical Implication and Managerial Implication

Theoretical Implication

This study extends vulnerability management literature by positioning resource constraints as structural conditions shaping governance capability in SMEs. The findings demonstrate that vulnerability management effectiveness depends not only on technological capability but also on managerial integration, governance coordination, and organizational learning. The study further conceptualizes vulnerability management as a governance-oriented organizational capability embedded within accounting control systems, where the interaction between detection, evaluation, managerial decision-making, and adaptive learning strengthens sustainable accounting data security practices in resource-constrained SMEs.

Managerial Implication

This study provides practical guidance for SMEs in strengthening accounting data security under limited resources. SMEs are encouraged to implement cost-efficient vulnerability assessment practices, establish internal security coordination, conduct regular risk evaluations, and strengthen employee security awareness through continuous training. The proposed model offers a practical framework for integrating vulnerability management into organizational governance and improving sustainable security capability in SMEs.

Conclusion and Future Direction

Conclusion

This study concludes that vulnerability management effectiveness in SMEs is shaped by technological capability and by integrating managerial coordination, governance structures, and organizational learning within accounting data security practices. The findings demonstrate that resource constraints influence how SMEs identify vulnerabilities, evaluate risks, and implement security responses. SMEs with stronger governance capability tend to institutionalize vulnerability management through structured tracking, cross-functional coordination, formalized policies, and continuous learning practices.

The proposed model consists of four interconnected parts: identification and detection, evaluation and prioritization, managerial decision integration, and HR awareness and continuous learning. These components run through a continuous feedback mechanism that strengthens adaptive governance and organizational resilience in resource-constrained SMEs.

Future Research Direction

Future research may apply quantitative or mixed-method approaches to confirm the proposed model across broader organizational and industrial contexts. Further studies may also examine how institutional environments, digital maturity, leadership, organizational culture, and emerging technologies influence vulnerability management and sustainable cybersecurity capability in SMEs.

References

Adejumo, A. P., & Ogburie, C. P. (2025). Strengthening Finance with Cybersecurity: Ensuring Safer Digital Transactions. *World Journal of Advance Reserach and Review*, *25*(March), 1527–1541. https://doi.org/10.30574/wjarr.2025.25.3.0908

Bennouk, K., & Aali. (2024). A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies. *Journal of Cybersecuryty and Privacy*, 853–908. https://doi.org/10.3390/jcp4040040

Bouncken, R. B., Czakon, W., & Schmitt, F. (2025). Purposeful Sampling and Saturation in Qualitative Research. *Review of Managerial Science*, 1–64. https://doi.org/10.1007/s11846-025-00881-2

Chotia, V., Khoualdi, K., Broccardo, L., & Zafar, M. (2025). Technology in Society The Role of Cyber Security and Digital Transformation in Gaining Competitive Advantage Through Strategic Management Accounting. *Technology in Society*, *81*(February), 102851. https://doi.org/10.1016/j.techsoc.2025.102851

Eisenhardt, K. M., & Bourgeois, L. J. (1988). Politics of Strategic Decision Making in High-Velocity Environments: Toward a Midrange Theory. *Academy of Management Journal*, *31*(4), 737–770. https://doi.org/10.5465/256337

Eisenhardt, K. M., Graebner, M. E., Eisenhardt, K. M., & Graebner, M. E. (2007). Theory Building from Cases: Opportunities and Challenges. *The Academyof Management Journal*, *50*(1), 25–32. https://psycnet.apa.org/doi/10.5465/AMJ.2007.24160888

Giudiece. (2024). *Methodologies and tools for a vulnerability management process with an integrated risk evaluation framework Author: Fortunato Gabriele Lo Giudice*.

Hollweck, T. (2016). Case Study Research Design and Methods. *The Canadian Journal of Program Evaluation*, *30*(2016), 1–5. https://doi.org/10.3138/cjpe.30.1.108

Isa, M., Praswati, A. N., & Zulaekah, S. (2024). Vulnerability Analysis: A Tool for SMEs ' Business Resilience. *Journal of Integrated Disaster Risk Management*, *14*, 157–175. https://doi.org/10.5595/001c.125616

Jiang, W., Almaayah, M., & Shehab, R. (2025). *Natural Language Processing-Driven Communication for Improved Citizen Alignment in Smart Cities*. 21–28. https://doi.org/10.70470/ESTIDAMAA/2025/003

Jiang, Y., Nay, Meng, Q., Lim, H. W., & Sikdar, B. (2025). A Survey on Vulnerability Prioritization: Taxonomy, Metrics, and Research Challenges. *Cryptography and Security*, *1*(1), 1–32. https://doi.org/10.48550/arXiv.2502.11070

Mazzano. (2025). CyberESP An Integrated Cybersecurity Framework for SMEs. *Journal of Software: Evolution and Process*, *37*, 1–23. https://doi.org/10.1002/smr.70050

Morshed, A. (2025). Cybersecurity in Digital Accounting Systems: Challenges and Solutions in the Arab Gulf Region. *Journal of Risk and Financial Management*, *18*(41), 1–24. https://doi.org/10.3390/jrfm18010041

Neri, M., Niccolini, F., & Pugliese, R. (2022). Assessing SMEs ' Cybersecurity Organizational Readiness: Findings From an Italian Survey. *Journal of Applied Knowledge Management*, *10*(September), 1–22. https://doi.org/10.36965/OJAKM.2022.10(2)1-22

Nurwanah. (2024). Advances in Applied Accounting Research Cybersecurity in Accounting Information Systems: Challenges and Solutions. *Advance in Apllied Accounting Reserach*, *2*(3), 157–168. https://doi.org/10.60079/aaar.v2i3.336%20Advances

Ridder. (2017). The Theory Contribution of case Study Research Designs. *Business Research*, *10*(2), 281–305. https://doi.org/10.1007/s40685-017-0045-z

Roup, A., & Effendy, M. (2025). Risk Analysis of Accounting Information System Security Based on Vulnerability Data From OPENVAS, OWASP ZAP, And NMAP Tools: A Cybersecurity Perspective. *Jurnal Ilmiah Akuntansi Kesatuan*, *13*(3), 433–438. https://doi.org/10.37641/jiakes.v13i3.3590

Rusu, D., & Mantulescu, M. (2025). Development of an Application-Based Framework for Information Security Management in SMEs. *Sustainability*, *17*(8314), 1–22. https://doi.org/10.3390/su17188314

Schilirò. (2024). Digital Transformation and its Impact on Organizations. *International Journal of Business and Management*, *19*(6), 71–81. https://doi.org/10.5539/ijbm.v19n6p71

Shimizu, N., & Hashimoto, M. (2025). Vulnerability Management Chaining: An Integrated Framework for Efficient Cybersecurity Risk Prioritization. *Cryptography and Security*, 1–16. https://doi.org/10.48550/arXiv.2506.01220

Thomann, & Maggetti, M. (2020). With Qualitative Comparative Analysis (QCA): Approaches , Challenges, and Tools. *Sociological Method & Reserach*, *49*(2). https://doi.org/10.1177/0049124117729700

Waweru, E., Karume, S. M., & Kibet, A. (2025). A Review of Human Vulnerabilities in Cyber Security: Challenges and Solutions for Microfinance Institutions. *Journal of Information Security*, *16*(1), 114–130. https://doi.org/10.4236/jis.2025.161006

Wijayanti, A. (2018). Factors Contributing Online Family Business To Enhance The Sustainability of Family Business. *The Turkish Online Journal of Design, Art and Communication*, (September), 3114–3120.

Yin, R. K. (2007). *Case study research: Design and methods* (3. ed., [Nachdr.]). Sage.

Yin, R. K. (2011). *How to Know Whether and When to Use The Case Study as A Reserach Method.*

Zlati, M. L., Ionescu, R. V., & Antohi, V. M. (2022). Modelling the Vulnerability of Financial Accounting Systems during Global Challenges: A Comparative Analysis. *Mathematics*, *10*(1462), 1–21. https://doi.org/10.3390/math10091462