Asean International Journal of Business

Vol.6 No.1 (2026)
e-ISSN: 2809-6673
pp.91-105

Strategic Outsourcing in the Digital Age: Cyber Risk Management and Operational Performance in Malaysian BPOs

Ferdio Ghifary Fidhien, Dodie Tricahyono*, Edi Witjara
Master of Management Program, School of Economics and Business, Telkom University, Indonesia
Corresponding Author: *dodietricahyono@telkomuniversity.ac.id

DOI: https://doi.org/10.54099/aijb.v5i1.1386

ARTICLE INFO

Research Paper

Article history:
Received: 12 June 2025
Revised: 1 January 2026
Accepted: 12 February 2026

Keywords: Business Process Outsourcing (BPO), Outsourcing Strategy, Data Security, Fraud Risk, Cyber Threat, Operational Performance, Good Governance

ABSTRACT

Business Process Outsourcing firms have become integral to Malaysia's post pandemic digital economy by providing non-core services such as information technology support, customer service, and business process administration. Alongside this growth, BPO firms face increasing exposure to data security breaches, fraud risk, and cyber threats, raising concerns about operational performance and governance quality. This study examines the effects of outsourcing strategy, data security, fraud risk, and cyber threats on the operational performance of Malaysian BPO firms listed on Bursa Malaysia during the 2021 to 2024 period, and analyzes the implications of operational performance for good governance. Using a quantitative explanatory design and Partial Least Squares Structural Equation Modeling, the study finds that outsourcing strategy and data security have significant positive effects on operational performance, while fraud risk and cyber threats exert significant negative effects. The results further demonstrate that operational performance positively influences good governance and mediates the relationship between outsourcing strategy, digital risk factors, and governance outcomes. The study contributes theoretically by integrating fraud risk and cyber threat into an outsourcing performance governance framework, thereby extending agency and stakeholder perspectives in digital outsourcing contexts. Practically, the findings offer insights for managers and regulators on aligning outsourcing decisions with digital risk management and governance practices to enhance accountability, transparency, and operational resilience in the BPO sector.

INTRODUCTION

Business Process Outsourcing (BPO) has become a cornerstone of operational efficiency for companies globally. In Malaysia, BPO firms classified under the Multimedia Super Corridor play a critical role in delivering specialised non-core services such as customer support, IT operations, and administrative processing. As digital transformation accelerates in the post-pandemic era, Malaysian BPO firms are projected to make significant contributions to national economic growth (Hori, 2023; Hayashi, 2023).Despite these opportunities, BPO companies face increasing threats related to data breaches, internal fraud, and cybersecurity risks (Jouini et al., 2014; Zhang et al., 2021). Moreover, as firms increasingly outsource their operations, ensuring alignment with good corporate governance principles becomes more challenging yet essential (OECD, 2004; Azizah et al., 2024). Weak internal controls and insufficient risk management mechanisms can undermine transparency, accountability, and stakeholder trust, thereby exposing organisations to heightened operational and governance risks (Freeman, 1984; Dorminey et al., 2012).This study focuses on how outsourcing strategies, data security, fraud risk management, and cyber threats influence the operational performance of BPO companies in Malaysia. It also examines the extent to which improved operational performance contributes to the implementation of good governance. By focusing on BPO firms listed on Bursa Malaysia during the 2021 to 2024 period, this research responds to the growing need for empirical evidence within an industry that plays a strategic role in the digital economy yet remains underexplored in governance and risk management studies (McIvor, 2009; Mehta et al., 2020).

In recent years, the BPO industry has experienced accelerated transformation driven by global digitisation and increasing client complexity. In emerging markets such as Malaysia, BPO firms have become critical enablers of cost efficiency, agility, and scalable service delivery across multiple sectors. However, reliance on third-party vendors has amplified concerns related to data protection, cybersecurity, and ethical vulnerabilities. Regulatory reports and governance studies increasingly highlight that BPO firms face heightened exposure not only to technological disruption but also to governance lapses and fraud incidents that are frequently underreported or institutionally overlooked (OECD, 2004; Azizah et al., 2024). These conditions underscore the need for a more integrated examination of operational risk and governance within digital outsourcing environments.Although prior research has examined the strategic and operational dimensions of outsourcing (McIvor, 2009; Mehta et al., 2020), limited empirical work has incorporated behavioural and integrity-based risks, particularly fraud risk and cyber threats, within the BPO context (Dorminey et al., 2012; Jouini et al., 2014; Zhang et al., 2021). Moreover, existing studies often position good governance as a contextual or antecedent factor rather than as an outcome shaped by operational performance, especially in information-intensive and high-risk service environments (OECD, 2004; Freeman, 1984). From a theoretical perspective, this creates an incomplete understanding of how agency problems, stakeholder accountability, and risk governance interact within outsourced digital ecosystems. Practically, BPO firms and regulators continue to face challenges in aligning outsourcing strategies with effective digital risk mitigation and governance implementation amid escalating cybersecurity incidents and fraud exposure (Azizah et al., 2024).Accordingly, this study aims to (1) examine the effects of outsourcing strategy, data security, fraud risk, and cyber threats on the operational performance of Malaysian BPO firms; (2) analyse the impact of operational performance on good governance; and (3) investigate the mediating role of operational performance in the relationship between digital risk factors and governance outcomes. The novelty of this research lies in its integrated risk performance governance framework, which simultaneously incorporates fraud risk and cyber threat constructs into a BPO outsourcing model and empirically positions operational performance as a governance enabling mechanism. By focusing on BPO firms listed on Bursa Malaysia, this study provides context-specific empirical insights that remain underexplored in the existing outsourcing, digital risk, and governance literature.

LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

Outsourcing Strategy

Outsourcing decisions are primarily grounded in Agency Theory and Transaction Cost Theory. Agency Theory explains outsourcing as a mechanism to reduce agency conflicts by transferring non-core activities to specialized external providers (Jensen & Meckling, 1976). Transaction Cost Theory further argues that firms outsource when external coordination costs are lower than internal governance costs (Williamson, 1979). Through outsourcing, organizations seek cost efficiency, access to specialized expertise, and enhanced operational flexibility.

McIvor (2009) identifies cost efficiency, access to external capabilities, and strategic focus as key dimensions of effective outsourcing strategies. Empirical studies further demonstrate that well-aligned outsourcing strategies enhance organizational agility and competitiveness, particularly in service-based industries operating in dynamic environments (Suresh & Ravichandran, 2022).

Data Security

Data security is rooted in Information Risk Management Theory, which conceptualizes information security as a systematic process of identifying, assessing, and mitigating risks associated with organizational data assets (Blakley et al., 2001). Contingency Theory complements this view by emphasizing that security mechanisms must be aligned with organizational context, technological complexity, and risk exposure.

Effective data security encompasses confidentiality, integrity, availability, authentication, and non-repudiation of information (Whitman & Mattord, 2011; Bandyopadhyay et al., 2010). In digital outsourcing environments, weak data protection exposes firms to service disruptions, reputational damage, and regulatory sanctions. Recent studies highlight the role of advanced technological solutions, including blockchain-based auditing and cloud assurance mechanisms, in strengthening data security governance (Mishra et al., 2021).

Fraud Risk Management

Fraud risk management is traditionally explained through the Fraud Triangle Theory, which identifies pressure, opportunity, and rationalization as key drivers of fraudulent behaviour (Cressey, 1953). The Fraud Diamond Theory extends this framework by incorporating individual capability as an additional determinant of fraud occurrence (Dorminey et al., 2012). The COSO framework further emphasizes internal control systems as the primary mechanism for fraud prevention and detection.

In BPO firms, fraud risk is amplified by high transaction volumes, multi-client data environments, and reliance on temporary or rotating labour forces. These structural characteristics increase opportunities for misconduct and complicate monitoring processes. Consequently, fraud risk in BPO contexts is not merely an internal governance concern but a direct threat to service quality, contractual compliance, and client trust. Prior studies confirm that ineffective fraud risk management undermines operational performance and governance credibility (Dorminey et al., 2012; Mehta et al., 2020; Azizah et al., 2024; Arifin & Koerniawan, 2025).

Cyber Threats

Cyber threats are a central concern in information security theory, which posits that unmanaged digital threats disrupt business continuity and operational resilience (Anderson, 2003). In BPO ecosystems, cyber risks such as phishing, malware, and denial of service attacks are increasingly prevalent due to extensive data sharing and decentralized operational structures (Jouini et al., 2014).

Empirical evidence suggests that cyber threats negatively affect operational efficiency by causing system downtime, data breaches, and reputational losses (Zhang et al., 2021; Wu et al., 2024). Despite this, many outsourcing studies treat cybersecurity as a peripheral IT issue rather than as a core performance determinant. Integrating cyber threat exposure into operational analysis is therefore critical, particularly for digital-first service industries such as BPOs. Governance-driven cybersecurity frameworks have been shown to mitigate these risks when properly enforced (Mishra et al., 2021; Piacenza et al., 2021).

Good Governance

Good governance is grounded in Stakeholder Theory, which emphasizes accountability, transparency, and responsibility toward diverse stakeholder groups (Freeman, 1984). The OECD principles further define governance quality through fairness, disclosure, and effective control mechanisms (OECD, 2004). Prior studies demonstrate that strong governance structures enhance long-term organizational performance and institutional trust (Aguilera & Cuervo Cazurra, 2009).

Empirical evidence from Malaysian institutions confirms that governance effectiveness is closely linked to accountability practices at the operational level (Azizah et al., 2024). In service-oriented industries, governance outcomes are not only shaped by board structures but also by frontline operational systems that support monitoring, reporting, and risk escalation.

Outsourcing Strategy and Operational Performance

Agency Theory and Transaction Cost Theory suggest that strategic outsourcing reduces coordination inefficiencies and allows firms to concentrate on core competencies. Empirical studies show that outsourcing strategies enhance operational flexibility, productivity, and service quality (McIvor, 2009; Suresh & Ravichandran, 2022). Therefore, the following hypothesis is proposed:
H1: Outsourcing strategy positively affects operational performance.

Data Security and Operational Performance

Effective data security ensures the confidentiality, integrity, and availability of organizational information, thereby minimizing operational disruptions and enhancing customer trust (Blakley et al., 2001; Whitman & Mattord, 2011). Empirical findings indicate that strong data protection frameworks contribute positively to operational stability and performance (Bandyopadhyay et al., 2010; Mishra et al., 2021). Hence:
H2: Data security positively affects operational performance.

Fraud Risk and Operational Performance

Fraud risk management is grounded in the Fraud Triangle Theory, which identifies pressure, opportunity, and rationalization as the primary drivers of fraudulent behaviour (Cressey, 1953), and is further reinforced by the COSO framework, which emphasises the role of internal control systems in preventing and detecting fraud (COSO, 2013). Strong internal controls reduce opportunities for fraud by limiting discretionary behaviour and strengthening monitoring mechanisms. Empirical evidence also highlights the role of individual capability and rationalisation in influencing fraud occurrence and its impact on organisational outcomes (Dorminey et al., 2012).

Existing research frequently associates fraud risk with weak internal controls or deficient ethical cultures, particularly within the public sector and financial institutions. However, the Business Process Outsourcing industry presents distinct structural vulnerabilities due to its reliance on transient labour forces, high transaction volumes, and multi-client data environments. These characteristics increase exposure to fraudulent behaviour and complicate detection and mitigation processes. In BPO firms, fraud risk extends beyond internal governance concerns, as fraudulent incidents directly affect service quality, contractual compliance, and client trust. Consequently, fraud risk represents not only an operational hazard but also a strategic governance issue, particularly in sectors where fiduciary responsibilities are delegated to third-party service providers (Dorminey et al., 2012; Mehta et al., 2020; Azizah et al., 2024; Arifin & Koerniawan, 2025). Therefore, the following hypothesis is proposed:
H3: Fraud risk negatively affects operational performance.

Cyber Threat and Operational Performance

Cyber threats are central to Information Security Theory, which posits that unmanaged digital threats disrupt business continuity and undermine organisational resilience (Anderson, 2003). Empirical studies consistently demonstrate that cyber threats such as data breaches, ransomware, and phishing attacks negatively affect operational efficiency by causing system downtime, financial losses, and reputational damage (Zhang et al., 2021; Wu et al., 2024).

Within BPO environments, cyber threats pose both technical and reputational risks due to decentralised operational structures and extensive third-party data handling. These conditions heighten vulnerability to security breaches and identity theft. Despite this, a significant portion of outsourcing literature continues to treat cybersecurity as a peripheral information technology concern rather than as an integrated determinant of operational performance. This study reconceptualises cyber threat exposure as a core performance factor in digital-first service industries such as BPO. By incorporating cyber threats into the operational performance framework, this research underscores the importance of embedding information security governance within day-to-day operations, shifting organisational responses from reactive compliance toward proactive risk architecture (Anderson, 2003; Zhang et al., 2021; Wu et al., 2024; Mishra et al., 2021; Piacenza et al., 2021). Accordingly, the following hypothesis is formulated:
H4: Cyber threats negatively affect operational performance.

Operational Performance and Good Governance

The relationship between operational performance and good governance is strongly supported by Stakeholder Theory, which emphasises accountability, transparency, and responsibility toward stakeholders as essential governance principles (Freeman, 1984). The OECD principles of corporate governance further assert that effective governance is reflected in the organisation's ability to deliver reliable performance while ensuring appropriate control and disclosure mechanisms (OECD, 2004). Empirical studies demonstrate that strong operational performance enhances stakeholder confidence and supports the consistent implementation of governance practices (Aguilera & Cuervo Cazurra, 2009; Azizah et al., 2024).

Although good governance is traditionally examined through board structures and shareholder oversight, its operational foundations are often overlooked. In service-oriented industries such as BPO, governance outcomes are shaped by frontline operational systems, including performance monitoring, escalation procedures, and real-time risk reporting. By empirically linking operational performance metrics to governance quality, this study contributes to the growing discourse on governance implementation beyond formal structures. It responds to increasing academic and regulatory interest in how outsourcing firms can institutionalise ethical conduct, client transparency, and control assurance through daily operational practices (Aguilera & Cuervo Cazurra, 2009; OECD, 2004; Christiansson & Rentzhog, 2020; Peköz, 2025; Azizah et al., 2024). Thus, the following hypothesis is proposed:

H5: Operational performance positively affects good governance.

Outsourcing Strategy and Good Governance

Strategic outsourcing arrangements influence governance outcomes by enhancing transparency, clarifying accountability, and strengthening control over vendor relationships. When outsourcing strategies are aligned with governance objectives, firms are better positioned to monitor third-party activities and enforce compliance standards. Empirical evidence indicates that outsourcing practices integrated with governance frameworks contribute positively to governance effectiveness (Mehta et al., 2020). Accordingly, this study proposes the following hypothesis:

H6: Outsourcing strategy positively affects good governance.

METHODOLOGY

Research Design

This study adopts a quantitative, explanatory research design using Structural Equation Modeling with Partial Least Squares (SEM-PLS). SEM-PLS is particularly suitable for testing complex causal relationships among latent constructs in predictive research models and is widely recommended for studies involving small to medium sample sizes and non-normal data distributions (Hair et al., 2021; Hair et al., 2022). Compared to covariance-based SEM, PLS SEM prioritises variance explanation and is therefore appropriate for theory development in emerging research contexts, including governance and risk management in Business Process Outsourcing industries (Hair et al., 2022; Ghozali, 2023).

Population and Sample

The population of this study consists of Business Process Outsourcing companies listed on Bursa Malaysia during the 2021 to 2024 period. A purposive sampling technique was employed due to the industry-specific nature of the research and the need to ensure data availability and comparability across firms. Listed BPO firms were selected because they provide audited disclosures and structured governance information, which are essential for analysing operational performance and governance practices within regulated outsourcing environments.

Data Collection

Primary data were collected using structured questionnaires distributed via email and online survey platforms. The questionnaire items were measured using a five-point Likert scale ranging from strongly disagree to strongly agree. This approach enables the systematic capture of respondents' perceptions regarding outsourcing strategy, data security, fraud risk, cyber threat exposure, operational performance, and good governance practices.

To ensure content validity, measurement items were adapted from previously validated instruments and refined to suit the Malaysian BPO context. The questionnaire was reviewed by academic experts and industry practitioners prior to distribution to confirm clarity, relevance, and contextual appropriateness.

Measurement Model Specification

All latent constructs in this study, namely outsourcing strategy, data security, fraud risk, cyber threat, operational performance, and good governance, were modelled as reflective constructs in accordance with established measurement theory. Reflective specification was selected because the observed indicators are assumed to be manifestations of the underlying latent variables rather than formative components.

Measurement Model Evaluation

The assessment of the measurement model focused on validity and reliability testing. Convergent validity was evaluated using Average Variance Extracted, with values exceeding the recommended threshold of 0.50 indicating adequate convergence. Construct reliability was assessed using Composite Reliability and Cronbach's Alpha, with values above 0.70 confirming internal consistency (Hair et al., 2022).

Discriminant validity was examined using the Fornell-Larcker criterion and the Heterotrait Monotrait ratio. These procedures ensure that each construct is empirically distinct from other constructs in the model and measures a unique conceptual domain.

Structural Model Evaluation

The structural model was evaluated by examining path coefficients, coefficient of determination, and predictive relevance. The explanatory power of the model was assessed using R-squared values for endogenous constructs, while predictive relevance was evaluated using the Stone-Geisser Q-squared statistic obtained through the blindfolding procedure. Path significance was tested using a bootstrapping procedure with 5,000 resamples to ensure robust statistical inference (Hair et al., 2022).

Model fit was assessed using the Standardized Root Mean Square Residual, with values below 0.08 indicating acceptable model fit (Ghozali, 2023).

Mediation Analysis

Mediation analysis was conducted to examine the indirect effects of outsourcing strategy, data security, fraud risk, and cyber threat on good governance through operational performance. The significance of indirect effects was assessed using the bootstrapping approach, allowing for the identification of partial or full mediation effects within the structural model.

Methodological Rigor

The combination of rigorous measurement validation, structural model evaluation, and mediation testing ensures both the reliability of the measurement model and the validity of the structural relationships examined in this study. This methodological approach supports the robustness of the empirical findings and strengthens the credibility of the conclusions drawn.

RESULTS AND DISCUSSION

This section presents the results of the Partial Least Squares Structural Equation Modeling (PLS-SEM) analysis conducted using SmartPLS version 4.0. The analysis evaluates both the measurement model (outer model) and the structural model (inner model), including indicator reliability, construct validity, and hypothesis testing.

Measurement Model Evaluation

Convergent Validity

Convergent validity was assessed using indicator factor loadings and Average Variance Extracted (AVE). As presented in Table 1, all indicator loadings exceed the recommended threshold of 0.70, indicating satisfactory indicator reliability. In addition, AVE values for all constructs are above 0.50, confirming that each construct explains more than half of the variance of its indicators and thus demonstrates adequate convergent validity.

Table 1. Measurent Model Results (Factor Loadings, CR, and AVE)

Construct	Indicator	Loading	Composite Reliability (CR)	Average Variance Extracted (AVE)
Strategi Outsourcing	X1.1	0.82	0.90	0.69
	X1.2	0.79		
	X1.3	0.85		
	X1.4	0.76		
Data Security	X2.1	0.88	0.91	0.72
	X2.2	0.93		
	X2.3	0.86		
	X2.4	0.79		
	X2.5	0.81		
Fraud Risk	X3.1	0.81	0.89	0.66
	X3.2	0.78		
	X3.3	0.84		
	X3.4	0.77		
	X3.5	0.80		
Cyber Threat	X4.1	0.87	0.91	0.69
	X4.2	0.82		
	X4.3	0.85		
	X4.4	0.80		
	X4.5	0.83		
Operational Performance	Y1.1	0.89	0.93	0.73
	Y1.2	0.85		
	Y1.3	0.91		
	Y1.4	0.88		
	Y1.5	0.86		
Good Governance	Z1.1	0.84	0.92	0.70
	Z1.2	0.82		
	Z1.3	0.86		
	Z1.4	0.83		
	Z1.5	0.80		

Reliability Analysis

Construct reliability was evaluated using Composite Reliability (CR) and Cronbach's Alpha. As shown in Table 1, all CR values exceed the minimum threshold of 0.70, and Cronbach's Alpha values are also above 0.70. These results indicate satisfactory internal consistency and confirm that all constructs are reliably measured.

Discriminant Validity

Discriminant validity was assessed using the Fornell–Larcker criterion and the Heterotrait–Monotrait (HTMT) ratio. The square roots of AVE for each construct are greater than their respective inter-construct correlations, satisfying the Fornell–Larcker criterion. Furthermore, all HTMT values are below the conservative threshold of 0.85, confirming that each construct is empirically distinct and that discriminant validity is established.

Structural Model (Inner Model) Evaluation

Model Fit (Goodness of Fit)

The overall model fit was assessed using the Standardized Root Mean Square Residual (SRMR). The SRMR value of 0.06 is below the recommended threshold of 0.08, indicating that the proposed structural model demonstrates a good fit with the observed data.

4.2.2 Coefficient of Determination (R^2)

The coefficient of determination (R^2) was used to evaluate the explanatory power of the model. As presented in Table 3, operational performance achieves an R^2 value of 0.63, indicating strong explanatory power, while good governance records an R^2 value of 0.49, indicating moderate explanatory power. According to Hair et al. (2021), these values are considered substantial for predictive models.

Table 3. R-Square (R^2) Values of Endogenous Constructs

Construct	R^2	Interpretation
Operational Performance	0.63	Strong explanatory power
Good Governance	0.49	Moderate explanatory power

Source: Research Results (2025)

Effect Size (f^2)

Effect size (f^2) analysis was conducted to assess the relative contribution of each exogenous construct to the endogenous variables. The results indicate that the outsourcing strategy and data security exert medium effects on operational performance, while fraud risk and cyber threat exhibit small to medium negative effects. These magnitudes are consistent with Cohen's (1988) guidelines and suggest meaningful practical relevance.

Predictive Relevance (Q^2)

Predictive relevance was assessed using the Stone–Geisser Q^2 value obtained through the blindfolding procedure. All endogenous constructs exhibit Q^2 values greater than zero, indicating that the model possesses satisfactory predictive relevance.

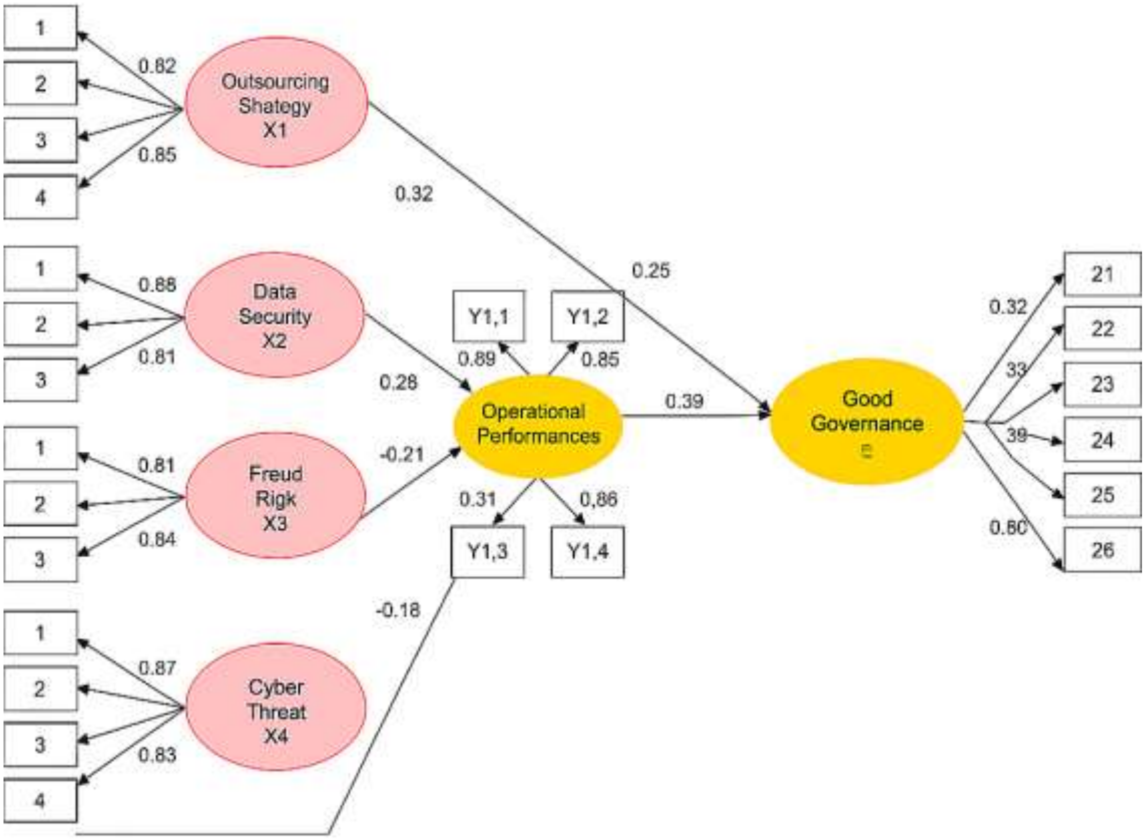

Figure 1. Structural Model of the Research Framework
Source: Research Results (2025)

Path Coefficient
The structural relationships among the constructs were examined through path coefficients, t-statistics, and p-values obtained from the bootstrapping procedure. As presented in Table 2, all hypothesised relationships are statistically significant at the 5 percent level.These results underscore the relevance of integrating operational drivers with governance outcomes, especially within high-risk, information-driven sectors such as BPO. The inclusion of fraud risk and cyber threat as key predictors expands the analytical scope of BPO performance modelling beyond the traditional efficiency and cost focus (Mehta et al., 2020; Christiansson & Rentzhog, 2020), providing empirical support for more comprehensive digital governance frameworks in outsourcing ecosystems.

Table 2. SEM Path Coefficients and Hypothesis Testing

Hypothesis	Relationship	Path Coefficient (β)	Description
H1	Outsourcing Strategy → Operational Performance	0.32	(Supported)
H2	Data Security → Operational Performance	0.28	(Supported)
H3	Fraud Risk → Operational Performance	-0.21	(Supported)
H4	Cyber Threat → Operational Performance	-0.18	(Supported)
H5	Operational Performance → Good Governance	0.39	Supported)
H6	Outsourcing Strategy → Good Governance	0.25	(Supported)

The results indicate that the outsourcing strategy and data security have significant positive effects on operational performance, while fraud risk and cyber threat exert significant negative effects. Operational performance, in turn, significantly enhances good governance. In addition, an outsourcing strategy has a direct positive effect on good governance.

The path coefficient analysis further confirms the hypothesised relationships. Outsourcing strategy and data security show significant positive effects on operational performance, supporting the view that strategic outsourcing and robust information protection enhance organisational efficiency (McIvor, 2009; Suresh & Ravichandran, 2022; Whitman & Mattord, 2011; Mishra et al., 2021). In contrast, fraud risk and cyber threat exhibit significant negative effects on operational performance, indicating that unmanaged integrity and cybersecurity risks undermine service quality and operational resilience (Dorminey et al., 2012; Wu et al., 2024). Operational performance demonstrates a strong positive effect on good governance, reinforcing the argument that governance quality is closely linked to the effectiveness of daily operations (Aguilera & Cuervo-Cazurra, 2009). Additionally, an outsourcing strategy has a direct positive effect on good governance, suggesting that transparent vendor management contributes to improved accountability and oversight (Mehta et al., 2020).

Discussion

The findings of this study highlight the strategic importance of outsourcing decisions and data security in shaping operational performance within Malaysian Business Process Outsourcing firms. The positive relationship between outsourcing strategy and operational performance supports the view that outsourcing is not merely a cost reduction mechanism but a strategic tool for enhancing organisational agility, specialisation, and resource allocation. This finding aligns with Agency Theory and Transaction Cost Theory, which posit that outsourcing reduces coordination inefficiencies and allows firms to focus on core competencies (Jensen & Meckling, 1976; Williamson, 1979). Consistent with prior empirical evidence, effective outsourcing strategies enable firms to improve flexibility and competitiveness in dynamic service environments (McIvor, 2009; Suresh & Ravichandran, 2022), a pattern also observed in regional BPO ecosystems in Asia (Hayashi, 2023; Hori, 2023).

Data security also emerges as a critical driver of operational performance, reinforcing the principle that organisational continuity depends on the protection of information confidentiality, integrity, and availability (Blakley et al., 2001; Whitman & Mattord, 2011). In data-intensive industries such as BPO, inadequate information security undermines client trust and exposes firms to operational disruptions (Bandyopadhyay et al., 2010). The findings lend support to recent studies that highlight the role of advanced security mechanisms, including blockchain-based auditing and externalised security frameworks, in mitigating digital risks and sustaining operational resilience (Mishra et al., 2021; Wu et al., 2024; Zhang et al., 2021).

In contrast, fraud risk and cyber threats exhibit significant negative relationships with operational performance, confirming that unmanaged integrity and cybersecurity risks erode organisational efficiency and reliability. This result is consistent with Fraud Triangle Theory and its extensions, which explain how opportunity, rationalisation, and capability contribute to fraudulent behaviour and organisational harm (Cressey, 1953; Dorminey et al., 2012). In the BPO context, where firms operate in high transaction volume and multi-client data environments, fraud and cyber incidents not only generate financial losses but also damage reputational capital and governance credibility (Arifin & Koerniawan, 2025). These findings reinforce prior evidence that proactive fraud surveillance and robust information technology governance are essential components of sustainable service delivery (Christiansson & Rentzhog, 2020; Singh et al., 2024).

The positive association between operational performance and good governance underscores the operational foundations of governance quality. Consistent with Stakeholder Theory and OECD governance principles, transparency, accountability, and responsibility are most effectively realised when daily operations are efficient, well monitored, and supported by reliable performance systems (Freeman, 1984; OECD, 2004; Aguilera & Cuervo-Cazurra, 2009). Evidence from Malaysian public institutions and state-owned enterprises further supports the argument that governance outcomes are closely linked to operational metrics and control practices at the unit level (Azizah et al., 2024). Moreover, the direct effect of outsourcing strategy on good governance suggests that transparent and well-governed vendor relationships strengthen oversight mechanisms and enhance stakeholder confidence (Mehta et al., 2020; Ghosh et al., 2016).

From a theoretical perspective, this study confirms the relevance of Agency Theory and Stakeholder Theory in explaining governance dynamics within digital outsourcing environments. By reducing information asymmetry and aligning incentives across internal and external actors, firms can simultaneously enhance operational efficiency and governance resilience (Freeman, 1984; Anwar et al., 2025). Comparable patterns have been observed in digital financial services and regional supply chain ecosystems, where outsourcing and risk management jointly underpin strategic performance (Salim et al., 2025; Ponciano & Amaral, 2021).

Methodologically, the use of Partial Least Squares Structural Equation Modelling strengthens the robustness of these theoretical insights by demonstrating substantial explanatory power for both operational performance and governance outcomes. This supports the argument that integrating an outsourcing strategy, data security, fraud risk, and cyber threat into a unified analytical framework provides a more comprehensive understanding of performance governance in BPO firms.

Finally, the findings offer practical contributions by outlining a governance-integrated outsourcing perspective for BPO practitioners. The results suggest that firms should move beyond efficiency-driven outsourcing models and embed risk-aware governance mechanisms into daily operations. This includes investments in cybersecurity infrastructure, internal fraud detection systems, and performance-based governance indicators that reinforce transparency and accountability. Such an approach is increasingly relevant for BPO leaders navigating digital transformation, knowledge management challenges, and technology-driven service delivery models (Peköz, 2025; Wong & Ngai, 2025; Yu, 2023; Zhong et al., 2025).

Overall, this study demonstrates that operational performance functions as a critical conduit through which outsourcing strategy and digital risk management shape governance quality. By positioning governance as an outcome of operational design and risk management rather than merely a compliance function, the findings provide meaningful insights for scholars, regulators, and practitioners operating within complex and technology-intensive outsourcing environments.

CONCLUSION

This study examined the effects of outsourcing strategy, data security, fraud risk, and cyber threats on operational performance and their implications for good governance within Malaysian Business Process Outsourcing firms. Using a Partial Least Squares Structural Equation Modeling approach, the findings demonstrate that strategic outsourcing and robust data security practices contribute positively to operational performance, while fraud risk and cyber threats exert detrimental effects. These results highlight that operational performance in BPO firms is shaped not only by strategic and technological choices but also by the effectiveness of integrity and risk management mechanisms.

The study further confirms that operational performance plays a mediating role in strengthening good governance. This finding suggests that governance quality is not solely determined by formal structures or compliance mechanisms, but is closely embedded in the effectiveness of daily operational processes. In the context of Malaysian BPO firms, governance emerges as an outcome of how well outsourcing strategies and digital risks are managed at the operational level.

From a theoretical perspective, this research reinforces the relevance of agency theory and stakeholder theory in digital outsourcing environments, while also extending resource-based perspectives by demonstrating how external partnerships and internal risk controls jointly influence performance and governance outcomes. By integrating fraud risk and cyber threat into the outsourcing performance model, the study contributes to a more comprehensive understanding of governance dynamics in information-intensive service industries.

Overall, the findings indicate that achieving sustainable governance in BPO firms requires more than efficiency-driven outsourcing decisions. Instead, firms must align outsourcing strategies with robust digital risk management and operational control systems, positioning governance as an integral outcome of operational design and strategic execution rather than a standalone compliance function.

IMPLICATIONS

The findings of this study generate several important implications for practice, regulation, and theory.

Managerial Implications.

For BPO executives, the results underscore the need to reconceptualise outsourcing as a strategic capability rather than a purely cost-driven decision. Effective outsourcing strategies must be supported by strong data security infrastructures and proactive fraud risk management to sustain operational performance. Managers should integrate cybersecurity controls, fraud detection mechanisms, and performance monitoring systems into daily operations to ensure that efficiency gains from outsourcing do not come at the expense of governance quality.

Governance and Regulatory Implications.

For regulators and stakeholders, the study highlights the importance of strengthening oversight frameworks for BPO firms operating in digital and data-intensive environments. Regulatory assessments should extend beyond formal governance disclosures to include evaluations of operational performance, digital risk exposure, and internal control effectiveness. Enforcing data protection standards, cybersecurity requirements, and outsourcing accountability mechanisms is critical for safeguarding trust and resilience in the BPO sector.

Theoretical Implications.

This research contributes to the literature by extending agency and stakeholder theories into the context of digital outsourcing and operational governance. By empirically linking operational performance to governance outcomes, the study supports a multi-layered view of firm resilience in which governance is shaped by strategic, technological, and operational factors simultaneously. This perspective enriches existing governance and outsourcing research in emerging digital economies.

LIMITATIONS AND FUTURE RESEARCH

Despite its contributions, this study is subject to several limitations. First, the use of cross-sectional data covering the 2021 to 2024 period limits the ability to make strong causal inferences regarding the relationships among outsourcing strategy, digital risks, operational performance, and governance. Longitudinal research designs could provide deeper insights into how these relationships evolve.

Second, the sample is limited to BPO firms listed on Bursa Malaysia, which may not fully represent smaller or non-listed outsourcing providers that operate under different governance and risk conditions. Future studies could expand the scope by including private firms or conducting comparative analyses across countries and regulatory environments.

Third, while SEM PLS is well-suited for predictive modelling and theory development, alternative methodological approaches such as covariance-based SEM or mixed methods designs may yield additional insights. Incorporating qualitative evidence through interviews or case studies could further enrich the understanding of how managers perceive and manage fraud and cyber risks in outsourcing contexts.

Future research may also explore additional moderating or mediating variables, such as organisational culture, digital maturity, or regulatory intensity, to refine the performance governance framework proposed in this study. Comparative studies across industries or regions would further enhance the generalisability and policy relevance of the findings.

REFERENCES

Aguilera, R. V., & Cuervo-Cazurra, A. (2009). Codes of good governance. Corporate Governance: An International Review, 17(3), 376-387.

Anderson, R. (2003). Security Engineering. Wiley.

Anwar, U.A.A., Rahayu, A., Wibowo, L.A. et al. Supply chain integration as the implementation of strategic management in improving business performance. Discov Sustain 6, 101 (2025). https://doi.org/10.1007/s43621-025-00867-w

Arifin, A. L. ., & Koerniawan, K. A. . (2025). Gender-diverse boards, liquidity, and financial distress: Pathways to fraud deterrence in auditor judgments. Edelweiss Applied Science and Technology, 9(5), 2549–2564. https://doi.org/10.55214/25768484.v9i5.7517

Azizah, W. ., Sudarmaji, E. ., & Khairany, N. . (2024). Good corporate governance at the unit level: Insights from a State-Owned Bank Branch. Edelweiss Applied Science and Technology, 8(6), 2544–2559. https://doi.org/10.55214/25768484.v8i6.2506

Bandyopadhyay, T., Jacob, V. & Raghunathan, S. Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. Inf Technol Manag 11, 7–23 (2010). https://doi.org/10.1007/s10799-010-0066-1

Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99-120.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. Proceedings of the 2001 Workshop on New Security Paradigms.

Christiansson, M.-T. and Rentzhog, O. (2020), "Lessons from the “BPO journey” in a public housing company: toward a strategy for BPO", Business Process Management Journal, Vol. 26 No. 2, pp. 373-404. https://doi.org/10.1108/BPMJ-04-2017-0091

Cressey, D. R. (1953). Other People's Money: A Study in the Social Psychology of Embezzlement.

Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley, R. A. (2012). The evolution of fraud theory. Issues in Accounting Education, 27(2), 555-579.

Freeman, R. E. (1984). Strategic Management: A Stakeholder Approach.

Ghosh, R., Gupta, A., Chattopadhyay, S., Banerjee, A. & Dasgupta, K. (2016). CoCOA: A Framework for Comparing Aggregate Client Operations in BPO Services. 2016 IEEE International Conference on Services Computing (SCC), San Francisco, CA, USA, 539-546. doi: 10.1109/SCC.2016.76.

Hailu, T. and Chebo, A.K. (2024), "Mapping business process outsourcing and innovation towards a future research", Business Process Management Journal, Vol. 30 No. 1, pp. 158-182. https://doi.org/10.1108/BPMJ-03-2023-0182

Hayashi, T. (2023). IT Business Process Outsourcing (BPO) Strategy as a New Development Strategy in Emerging Countries: Focusing on the Philippine IT-BPO Industry and Lewis Turning Point Theory. In: Hayashi, T., Hoshino, H., Hori, Y. (eds) Base of the Pyramid and Business Process Outsourcing Strategies. Springer, Singapore. https://doi.org/10.1007/978-981-19-8171-5_7

Hori, Y. (2023). The Growth of the IT-BPO Industry and Women’s Work Choices in the Philippines. In: Hayashi, T., Hoshino, H., Hori, Y. (eds) Base of the Pyramid and Business Process Outsourcing Strategies. Springer, Singapore. https://doi.org/10.1007/978-981-19-8171-5_6

Jayaprabha, D., & Nirmala, K. (2018). Efficiency stress prediction in BPO industries using hybrid k-means and artificial bee colony algorithm. International Journal of Computers and Applications, 42(1), 9–16. https://doi.org/10.1080/1206212X.2017.1396416

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm. Journal of Financial Economics, 3(4), 305-360.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. Procedia Computer Science, 32, 489-496.

Kaplan, R. S., & Norton, D. P. (1992). The balanced scorecard: Measures that drive performance. Harvard Business Review, 70(1), 71–79.

Kato, H., & Chihama, Y. (2010). Business operations integration/BPO service for regional financial institutions. NEC Technical Journal, 5(2), 38–44. https://www.scopus.com/inward/record.uri?eid=2-s2.0-77953993150&partnerID=40&md5=2df82d20e52a11f6e585ab8167d44734

McIvor, R. (2009). How the transaction cost and resource-based theories of the firm inform outsourcing evaluation. Journal of Operations Management, 27(1), 45-63.

Mehta, A. M., Hafeez, I., Ali, A., Rahi, S., & Saleem, H. (2020). Examining the influence of BPO risks, vendor team's performance, and knowledge management capability. Journal of Management Information and Decision Sciences, 23(Special Issue), 397–408. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85099521329&partnerID=40&md5=d46464b33cfff45aa59e8022dfaf38d0

Mishra, R., Ramesh, D. & Edla, D.R. Dynamic large branching hash tree based secure and efficient dynamic auditing protocol for cloud environment. Cluster Comput 24, 1361–1379 (2021). https://doi.org/10.1007/s10586-020-03193-0

OECD. (2004). Principles of Corporate Governance. Organisation for Economic Co-operation and Development.

Peköz, Ü.G. (2025). Knowledge Management and Business Processes in CEE Service Centers. In: Štarchoň, P., Fedushko, S., Gubíniova, K. (eds) Developments in Information and Knowledge Management Systems for Business Applications. Studies in Systems, Decision and Control, vol 578. Springer, Cham. https://doi.org/10.1007/978-3-031-80935-4_16

Piacenza, J. R., Faller, K. J., II, Regez, B., and Gomez, L. (April 30, 2021). Verification of Numerically Controlled Manufacturing Processes, Toward Identifying Cyber-Physical Threats. ASME. J. Manuf. Sci. Eng. September 2021; 143(9): 091014. https://doi.org/10.1115/1.4050547

Piacenza, J, Faller, KJ, II, Regez, B, & Gomez, L. (2020). Investigating Cyber-Physical Threats of Numerically Controlled Manufacturing Processes. Proceedings of the ASME 2020 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. Volume 6: 25th Design for Manufacturing and the Life Cycle Conference (DFMLC). V006T06A012. ASME. https://doi.org/10.1115/DETC2020-22324

Ponciano, E.S. and Amaral, C.S.T. (2021), What influences the innovation environment in BPO companies? Business Process Management Journal, Vol. 27 No. 1, pp. 106-123. https://doi.org/10.1108/BPMJ-03-2020-0129

Respati, N. P., & Tricahyono, D. (2020). Performance Analysis Using Balanced Scorecard Approach From Growth and Learning Perspective (Case Study at Muhammadiyah Hospital Bandung). e-Proceeding of Management, Vol.7, No.2, 2119-2120.

Salim, D. F. ., Candraningtias, W. ., Koerniawan, K. A. ., & Isynuwardhana, D. . (2025). Gender-inclusive fintech and economic growth: The case of P2P lending in Indonesia. Edelweiss Applied Science and Technology, 9(5), 424–435. https://doi.org/10.55214/25768484.v9i5.6885

Singh, L., Chirputkar, A., & Ashok, P. (2024). Risk Management in the Digital Age: Fintech Security Strategies. 2024 1st International Conference on Sustainable Computing and Integrated Communication in Changing Landscape of AI (ICSCAI), Greater Noida, India, 1-7. https://doi.org/10.1109/ICSCAI61790.2024.10866839

Suresh, S., & Ravichandran, T. (2022). Value Gains in Business Process Outsourcing: The Vendor Perspective. Information Systems Frontiers, 24, 677–690. https://doi.org/10.1007/s10796-021-10111-1

Szortyka, K. (2024). Intelligent automation of financial and accounting processes in business process outsourcing centers in Poland. ZTR, 48(3), 155-175. https://doi.org/10.5604/01.3001.0054.7261.

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security.

Wong, D. T. W., & Ngai, E. W. T. (2025). Impact of artificial intelligence (AI) on operational performance: The role of dynamic capabilities. Information & Management, 62(6), 104162. https://doi.org/10.1016/j.im.2025.104162

Wu, Y., Wang, N., Dai, T., & Cheng, D. (2024). Information security outsourcing strategies in the supply chain considering security externality. Journal of the Operational Research Society, 76(3), 482–497. https://doi.org/10.1080/01605682.2024.2368611

Yu, Y. (2023). Implementation and Assurance Model Construction of Financial BPO Cost Control under Cloud Computing Platform. Applied Mathematics and Nonlinear Sciences, 9(1), 2023. https://doi.org/10.2478/amns.2023.2.00134

Zhang, C., Feng, N., Chen, J., et al. (2021). Outsourcing Strategies for Information Security: Correlated Losses and Security Externalities. Information Systems Frontiers, 23, 773–790. https://doi.org/10.1007/s10796-020-10009-4

Zhong, W., Zhao, L., & Dou, Q. (2025). The Implementation Strategy of Cost Control and the Construction of a Guarantee Model of Financial BPO in the Cloud Computing Environment. International Journal of Information System Modeling and Design (IJISMD), 16(1), 1-21. https://doi.org/10.4018/IJISMD.367278