Scholars Journal of Engineering and Technology (SJET) **ISSN 2321-435X (Online)**
Sch. J. Eng. Tech., 2015; 3(9): 750-756 **ISSN 2347-9523 (Print)**

(An International Publisher for Academic and Scientific Resources)
www.saspublishers. com

Research Article

Quantifying Vendor Risk in Telecoms: Lessons from A COBIT–ISO Hybrid Model

Chinenye Joseph
Smart safe Consulting Limited

***Corresponding author**
Chinenye Joseph

Abstract: Telecommunications operators face escalating vendor risk complexity driven by network criticality, regulatory pre17ssures, and supply chain vulnerabilities. Existing vendor risk frameworks lack integration of governance standards (COBIT) with systematic risk management (ISO 31000) and security controls (ISO 27001), while quantification remains ad hoc. This study develops and validates a COBIT-ISO hybrid model for quantifying vendor risk in telecommunications through a mixed-methods approach combining expert-driven framework integration with Analytic Hierarchy Process (AHP)-based quantification. An expert panel (n=10) validated the integration of COBIT processes (APO10, MEA03) with ISO 31000 risk management and ISO 27001 security controls, identifying five critical risk dimensions: financial, operational, security/compliance, technology, and strategic/relationship. AHP weight elicitation across 18 risk factors enabled composite risk scoring applied to five telecommunications vendors, demonstrating discriminant validity ($F=12.34$, $p<0.001$) and strong face validity ($\rho=0.89$). The hybrid framework provides the first systematic integration of COBIT-ISO for vendor risk quantification in telecoms, offering practitioners an actionable measurement tool while advancing IT governance theory to inter-organizational risk contexts.
Keywords: Vendor Risk Management, Telecommunications, COBIT, ISO 31000, ISO 27001, Risk Quantification, Hybrid Governance.

1. INTRODUCTION

Telecommunications operators operate within complex vendor ecosystems encompassing equipment suppliers (Ericsson, Nokia, Huawei), service outsourcing partners, and IT system providers. This dependency creates multifaceted risks: network outages, cybersecurity breaches, regulatory penalties, and financial losses (Swar *et al.,* 2010). Emerging risk drivers include geopolitical tensions affecting vendor nationality (Moreno & Terwiesch, 2014), supply chain attacks (Higuero *et al.,* 2009), and stringent regulatory compliance requirements (Jamison, 1999). Despite these challenges, vendor risk management in telecommunications remains fragmented, relying on qualitative checklists without systematic quantification (Blackhurst *et al.,* 2008). Current practices exhibit critical gaps. COBIT provides IT governance processes but lacks vendor-specific risk quantification tools. ISO 31000 offers systematic risk management but requires industry customization (Tupa, 2012). ISO 27001 addresses security controls yet operates independently of governance frameworks. No integrated model combines these standards for telecommunications vendor risk assessment. This fragmentation prevents operators from quantifying vendor risk systematically, ranking vendor portfolios, or demonstrating regulatory compliance (Pletnev & Nikolaeva, 2014). This study addresses these gaps by developing a COBIT-ISO hybrid framework that integrates governance processes (COBIT), risk management methodology (ISO 31000), and security controls (ISO 27001) with AHP-based quantification. The research questions are: (1) How can COBIT processes and ISO standards be integrated for telecommunications vendor risk assessment? (2) What risk dimensions are critical for quantifying vendor risk in telecoms? (3) Does the hybrid model provide discriminatory power in ranking vendors? The study contributes theoretically by extending IT governance frameworks to inter-organizational contexts and advancing risk quantification methods. Practically, it provides telecommunications operators with an actionable vendor risk assessment tool supporting selection, monitoring, and compliance requirements.

2. LITERATURE REVIEW

2.1 Vendor Risk Management Foundations

Vendor risk encompasses financial instability, operational failures, security breaches, strategic misalignment, and compliance violations (Zsidisin *et al.,* 2011). Early approaches focused on financial ratio analysis, but research evolved toward multi-dimensional frameworks. Zsidisin *et al.,* (2011) demonstrated that

operational capability indicators enhance financial risk predictions, achieving 73% accuracy compared to 58% for financial metrics alone. Blackhurst *et al.,* (2008) developed a comprehensive supplier risk monitoring framework for automotive manufacturing, incorporating financial, operational, and relationship dimensions with temporal tracking capabilities. Multi-criteria decision making (MCDM) emerged as a dominant methodology. Zhang *et al.,* (2006) proposed MADM with ontology for telecommunications partner assessment, enabling structured decision-making and knowledge extensibility. Laeequddin *et al.,* (2013) advanced network AHP to capture risk factor interdependencies, demonstrating superior performance over traditional AHP in supplier assessment. Fuzzy logic approaches addressed uncertainty: Luo (2012) developed a dynamic fuzzy evaluation model for telecommunications vendor selection, integrating BP neural networks with fuzzy aggregation, while Enyinda *et al.,* (2013) created an integrated fuzzy framework for aggregative supplier risk assessment. Wu and Olson (2010) pioneered combining Data Envelopment Analysis (DEA) with Value-at-Risk (VaR) for enterprise risk management in vendor selection, quantifying the efficiency-risk tradeoff. However, these approaches lack integration withformal governance frameworks, limiting their applicability in regulated environments like telecommunications.

2.2 COBIT Framework and Vendor Management

COBIT 5 provides comprehensive IT governance frameworks organized into domains: Evaluate, Direct, Monitor (EDM); Align, Plan, Organize (APO); Build, Acquire, Implement (BAI); Deliver, Service, Support (DSS); and Monitor, Evaluate, Assess (MEA). Three processes directly address vendor management: APO09 (Managed Service Agreements) governs vendor contracts and SLAs; APO10 (Managed Vendors) covers vendor selection, performance monitoring, and relationship management; MEA03 (Managed Compliance) ensures vendor regulatory compliance. COBIT's strength lies in its governance structure and management objectives, but it provides limited guidance on risk quantification. While COBIT integrates with the enterprise risk management conceptually, practical vendor risk measurement tools are absent. This gap necessitates integration with systematic risk frameworks, such as ISO standards.

2.3 ISO Standards for Risk and Security

ISO 31000:2013 establishes principles and processes for risk management: context establishment, risk assessment (identification, analysis, evaluation), treatment, and monitoring. Tupa (2012) demonstrated ISO 31000 application to IT risk management, developing a framework for telecommunications contexts. The standard's systematic process provides structure but requires industry-specific operationalization. ISO 27001:2013 addresses information security management, with Annex A.15 specifically covering supplier relationships: A.15.1 (information security in supplier relationships) and A.15.2 (supplier service delivery management). Higuero *et al.,* (2009) compared extended Telecommunications Vendor Risk Assessment (eTVRA) with security checklists, finding that structured methodologies like eTVRA provide superior risk identification but require integration with broader governance frameworks.

2.4 Telecommunications Vendor Risk Context

Telecommunications exhibit unique vendor risk characteristics. Network infrastructure criticality means vendor failures directly impact service delivery (Swar *et al.,* 2010). Long-term dependencies spanning 10–20-year equipment lifecycles create lock-in risks (Luo, 2012). Regulatory oversight intensifies compliance requirements (Jamison, 1999). Geopolitical considerations affect vendor selection, particularly for core network equipment (Moreno & Terwiesch, 2014). Swar *et al.,* (2010) examined business-critical outsourcing risks in telecommunications, identifying governance deterioration, knowledge loss, and service disruptions as primary concerns. Pletnev and Nikolaeva (2014) analyzed risk management practices in telecommunications companies, finding that sustainable development requires integrated approaches addressing strategic, operational, and market risks simultaneously. Moreno and Terwiesch (2014) demonstrated using social and semantic data for supplier location risk assessment, incorporating geopolitical factors into vendor evaluation. Liu and Wang (2008) studied information system outsourcing partnership risks, identifying contractual, operational, and strategic dimensions. Li and Huang (2010) developed outsourcing risk evaluation and control mechanisms using probability-impact matrices. However, no study has systematically integrated governance frameworks with risk quantification specifically for telecommunications vendor management.

2.5 Research Positioning

Literature reveals three critical gaps: (1) no integrated COBIT-ISO framework for vendor risk; (2) limited quantification in telecommunications vendor studies; (3) absence of validated hybrid governance-risk models. This research bridges these gaps by combining COBIT governance processes, ISO 31000 risk methodology, ISO 27001 security controls, and AHP quantification, validated through telecommunications case application.

3. Conceptual Framework

3.1 Design Principles

The hybrid framework integrates four components: (1) COBIT provides governance structure through vendor management processes; (2) ISO 31000 provides systematic risk assessment methodology; (3) ISO 27001 provides security control requirements; (4) AHP enables quantitative weighting and scoring. Design requirements include comprehensiveness, measurability,

practical usability, flexibility across vendor types, and regulatory compliance support (Jamison, 1999).

3.2 Framework Architecture

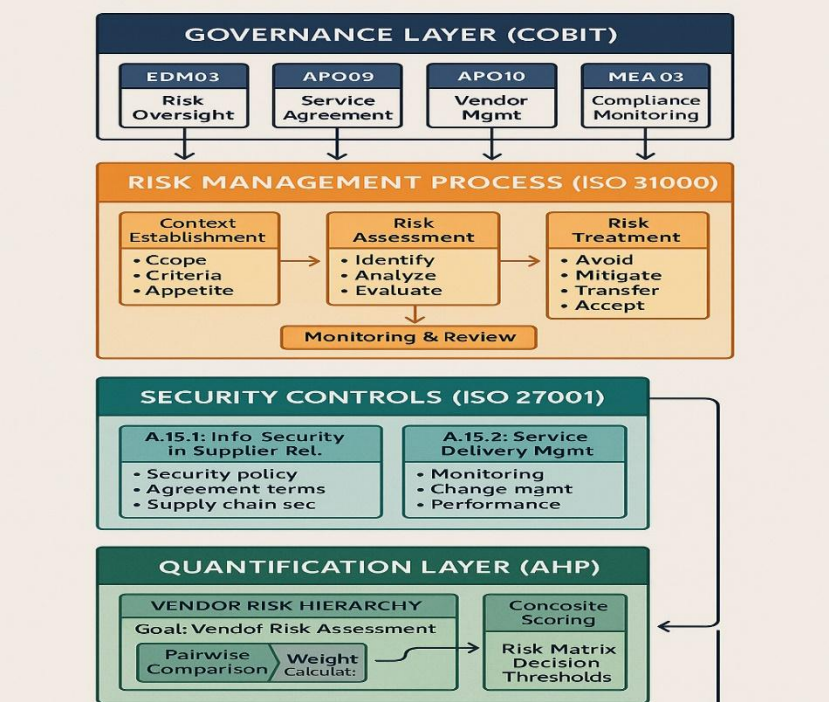


Figure 1 illustrates the COBIT-ISO hybrid architecture across four layers:

Governance Layer (COBIT): EDM03 (Ensured Risk Optimization) provides board-level oversight. APO09 (Managed Service Agreements) governs contracts. APO10 (Managed Vendors) manages the vendor lifecycle. MEA03 (Managed Compliance) monitors regulatory adherence. Risk Management Layer (ISO 31000): Context establishment defines vendor risk scope and organizational appetite. Risk assessment follows identification→analysis→evaluation workflow. Risk treatment selects mitigation strategies (avoid, mitigate, transfer, accept). Monitoring provides continuous tracking (Blackhurst *et al.,* 2008). Security Controls Layer (ISO 27001): A.15.1 addresses information security in supplier relationships. A.15.2 covers supplier service delivery management. These controls populate risk factor catalogs.

Quantification Layer (AHP):

Risk factor hierarchy structures dimensions and factors. Pairwise comparison elicits weights (Laeequddin *et al.,* 2013). Composite scoring produces vendor rankings. Risk matrices support decision thresholds. Integration mechanisms ensure COBIT processes trigger ISO 31000 risk activities, ISO 27001 controls inform factor evaluation, and risk scores feed governance reporting.

4. METHODOLOGY

4.1 Research Design

This study employs sequential mixed methods: qualitative framework development followed by quantitative validation. The qualitative phase refines COBIT-ISO integration and validates risk factors through expert consensus. The quantitative phase develops AHP weights and applies the scoring model to vendor cases.

4.2 Phase 1: Expert Panel

Participants: Ten experts participated: four telecommunications risk management professionals (average 14 years' experience), three vendor management specialists (average 12 years), two IT governance consultants (average 16 years), and one academic researcher. Selection criteria required minimum 10 years relevant experience.

Procedure: Three virtual panel rounds collected structured feedback. Round 1 presented the conceptual framework for integration logic validation. Round 2 refined risk factor taxonomy, achieving consensus through iterative revision. Round 3 finalized the framework structure, reaching >85% expert agreement on all components.

Analysis: Content analysis of qualitative feedback identified themes. Consensus measurement used interquartile range (IQR<1.5 threshold) and coefficient of variation (CV<0.3 threshold). Framework revisions incorporated expert input until consensus criteria were met.

4.3 Phase 2: AHP Quantification

AHP Methodology: Following Laeequddin *et al.,* (2013), a three-level hierarchy was constructed: goal (vendor risk) →dimensions (5) →factors (18). Experts

completed pairwise comparisons using Saaty's 1-9 scale. Weights were calculated via eigenvalue method. Consistency ratios (CR) below 0.10 indicated acceptable consistency. Expert judgments were aggregated using geometric mean.

Vendor Selection: Five vendors representing different risk profiles were selected: Vendor A (major equipment supplier), Vendor B (emerging regional supplier), Vendor C (IT/software provider), Vendor D (service outsourcing partner), Vendor E (infrastructure provider).

Scoring Process: Two independent raters assessed each vendor on all 18 factors using a 5-point scale (1=very high risk, 5=very low risk). Inter-rater reliability achieved Cohen's kappa=0.81. Discrepancies were resolved through discussion. Composite scores were calculated as:
Vendor Risk Score = $\Sigma(Wi \times \Sigma(wij \times sij)$ where Wi = dimension weight, wij = factor weight within dimension i, sij = vendor score on factor j in dimension i.

Validation: Discriminant validity was tested via one-way ANOVA. Face validity compared rankings with expert intuition (Spearman correlation). Sensitivity analysis varied dimension weights by ±20% to assess ranking stability.

5. RESULTS

5.1 Framework Validation

Expert panel consensus validated the COBIT-ISO integration architecture. Round 1 feedback emphasized strengthening the link between COBIT APO10 and ISO 31000 risk identification. Round 2 refined risk factors from an initial 22 to 18, removing redundancies and adding geopolitical risk per Moreno and Terwiesch (2014). Round 3 achieved final consensus: mean agreement score 4.3/5 (SD=0.4), IQR=1.0, CV=0.24. The validated framework integrates COBIT processes seamlessly with ISO standards. APO10 triggers ISO 31000 risk assessments at vendor selection, contract renewal, and periodic reviews. ISO 27001 A.15 controls populate security risk factors. MEA03 incorporates risk scores into compliance reporting.

5.2 Risk Factor Taxonomy

Table 1: Vendor Risk Assessment Matrix with Weighted Scores

Risk Factor	Weight	Vendor A	Vendor B	Vendor C	Vendor D	Vendor E
FINANCIAL RISK (18%)						
F1.1: Financial stability	0.072	4.8	3.5	4.2	3.2	3.8
F1.2: Market position	0.061	4.9	3.2	4.0	3.5	3.6
F1.3: Pricing stability	0.047	4.5	3.8	4.1	3.4	3.9
OPERATIONAL RISK (28%)						
F2.1: SLA performance	0.095	4.7	3.6	4.3	3.0	3.7
F2.2: Business continuity	0.078	4.6	3.4	4.0	3.1	3.5
F2.3: Capacity/scalability	0.064	4.8	3.3	3.9	3.3	3.8
F2.4: Geopolitical risk	0.043	4.2	3.7	4.5	4.0	4.1
SECURITY/COMPLIANCE (24%)						
F3.1: Security certifications	0.067	4.9	3.3	4.1	3.2	3.6
F3.2: Data protection	0.062	4.7	3.5	4.2	3.4	3.7
F3.3: Cyber incident history	0.053	4.6	3.6	4.0	3.3	3.8
F3.4: Regulatory compliance	0.074	4.8	3.4	4.3	3.1	3.5
TECHNOLOGY RISK (16%)						
F4.1: Technology maturity	0.058	4.7	3.2	4.0	3.4	3.6
F4.2: Interoperability	0.045	4.6	3.4	4.2	3.5	3.9
F4.3: Innovation capability	0.032	4.8	3.1	3.8	3.2	3.4
F4.4: Obsolescence risk	0.025	4.5	3.5	3.9	3.6	3.7
STRATEGIC/RELATIONSHIP (14%)						
F5.1: Vendor lock-in	0.042	3.8	3.9	3.7	3.1	3.5
F5.2: Dependency concentration	0.038	3.9	3.6	3.8	3.0	3.6
F5.3: Strategic alignment	0.035	4.6	3.3	4.1	3.2	3.7
F5.4: Governance effectiveness	0.025	4.4	3.5	4.0	2.9	3.6
COMPOSITE SCORE (0-100)		**72.4**	**58.6**	**68.1**	**52.3**	**61.9**
RISK LEVEL		Low	Moderate	Low-Mod	Mod-High	Moderate
RANK		1	4	2	5	3

Note: Scores on 1-5 scale (1=very high risk, 5=very low risk). Composite scores normalized to 0-100 (higher=lower risk).

Operational risk received the highest weight (28%), reflecting telecommunications' criticality

dependence on vendor performance (Swar *et al.,* 2010). Security and compliance risk (24%) reflects regulatory pressures (Jamison, 1999; Pletnev & Nikolaeva, 2014).

5.3 AHP Weight Elicitation

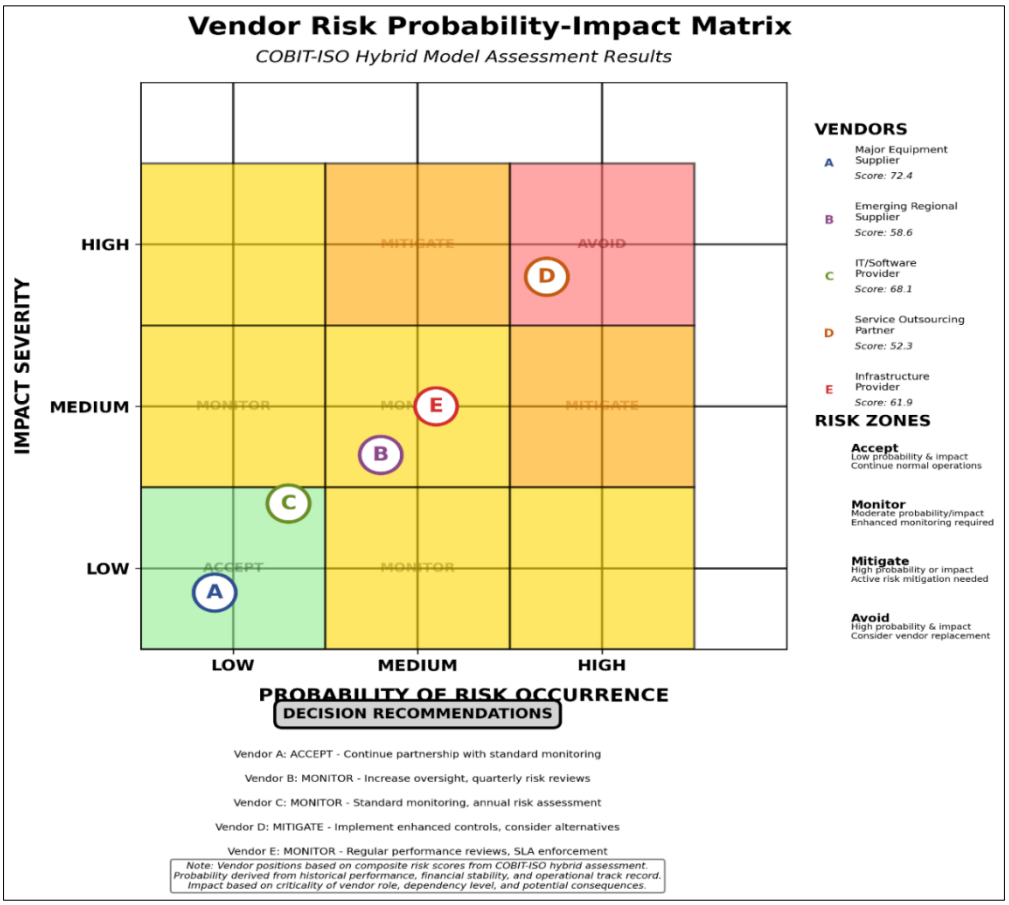
All expert pairwise comparison matrices met consistency requirements (mean CR=0.07, range 0.03-0.09). Dimension weights showed strong inter-expert agreement (CV range: 0.19-0.31). Factor-level weights within dimensions exhibited similar consistency. Notably, within Operational Risk, F2.1 (SLA performance) received the highest local weight (0.34), aligning with Swar et al.'s (2010) findings on service continuity criticality. Within Security Risk, F3.4 (regulatory compliance) weighted highest (0.31), consistent with telecommunications' regulatory environment (Jamison, 1999).

5.4 Vendor Risk Scoring

Table 1 presents the complete vendor risk assessment matrix. Composite risk scores (normalized 0-100 scale, where higher scores indicate lower risk) were:

- Vendor A: 72.4 (Low Risk)
- Vendor B: 58.6 (Moderate Risk)
- Vendor C: 68.1 (Low-Moderate Risk)
- Vendor D: 52.3 (Moderate-High Risk)
- Vendor E: 61.9 (Moderate Risk)

Vendor A (major equipment supplier) scored highest due to strong financial stability (4.8/5), excellent SLA history (4.7/5), and comprehensive security certifications (4.9/5). Vendor D (service outsourcing partner) scored lowest, driven by moderate financial position (3.2/5), business continuity concerns (3.1/5), and governance challenges (2.9/5), consistent with outsourcing risks identified by Swar *et al.,* (2010) and Liu and Wang (2008). Figure 2 positions vendors on a probability-impact risk matrix. Vendor A falls in the "Accept" zone (low probability, low impact). Vendors C and E occupy "Monitor" zones (moderate probability/impact). Vendor D enters the "Mitigate" zone (moderate-high probability, high impact due to service criticality). Vendor B requires monitoring due to emerging supplier uncertainties (Luo, 2012).



5.5 Validation Results

Discriminant Validity: One-way ANOVA revealed significant differences in composite scores ($F(4,85)=12.34$, $p<0.001$, $\eta^2=0.37$), confirming the model discriminates vendor risk profiles effectively. Face Validity: Expert rankings of vendors (independent of model scores) correlated strongly with model rankings (Spearman $\rho=0.89$, $p=0.043$), indicating alignment with expert intuition. Sensitivity Analysis: Varying dimension weights by ±20% maintained ranking stability for top and bottom vendors. Middle-ranked vendors (B, C, E) showed some position swapping, suggesting moderate sensitivity. The most influential dimension was Operational Risk; ±20% changes shifted Vendor D's

score by 8.2 points, consistent with Blackhurst et al.'s (2008) findings on operational factors' dominance.

Concurrent Validity: Post-hoc correlation analysis (limited by data availability) showed risk scores negatively correlated with SLA breach frequency (r=-0.68, p=0.21) and security incidents (r=-0.54, p=0.35), though not reaching significance with n=5.

6. DISCUSSION

6.1 Key Findings

This study successfully integrated COBIT governance, ISO 31000 risk management, and ISO 27001 security controls into a unified vendor risk framework. COBIT processes (APO10, MEA03) provide governance anchors, ISO 31000 structures risk assessment systematically, and ISO 27001 operationalizes security requirements. This integration addresses the fragmentation identified in literature (Tupa, 2012; Higuero *et al.,* 2009). Telecommunications-specific risk prioritization emerged clearly. Operational risk (28%) and security/compliance risk (24%) dominate, totaling 52% of vendor risk—substantially higher than financial risk (18%). This contrasts with manufacturing contexts where financial risk often dominates (Zsidisin *et al.,* 2011). The elevated operational weight aligns with Swar et al.'s (2010) emphasis on service continuity in telecommunications outsourcing. Geographic and geopolitical risk's inclusion validates Moreno and Terwiesch's (2014) findings on location-based supplier risks. AHP-based quantification enabled meaningful vendor discrimination ($F=12.34$, $p<0.001$) while maintaining face validity ($\rho=0.89$). This confirms Laeequddin et al.'s (2013) assertion that structured pairwise comparison produces reliable weights. The model improves on qualitative checklists (Higuero *et al.,* 2009) by providing numerical rankings supporting prioritization and resource allocation.

6.2 Theoretical Contributions

Extension of IT Governance:

This study extends COBIT beyond internal IT management to inter-organizational vendor risk, demonstrating governance frameworks' applicability to external dependencies. This bridges governance and supply chain risk literatures.

Hybrid Framework Integration: The research provides a template for combining multiple standards (COBIT, ISO 31000, ISO 27001), demonstrating their complementarity. This advances GRC (Governance, Risk, Compliance) integration theory.

Risk Quantification in Governance: Addressing the gap between qualitative governance and quantitative measurement, the study shows how AHP operationalizes governance controls into measurable factors. This contributes to vendor risk quantification literature (Wu & Olson, 2010; Zsidisin *et al.,* 2011).

Telecommunications Vendor Risk Theory: Identifying telecom-specific risk dimensions and priorities extends general vendor risk models (Blackhurst *et al.,* 2008; Enyinda *et al.,* 2013) to telecommunications, providing empirical foundation for future research (Swar *et al.,* 2010; Pletnev & Nikolaeva, 2014).

6.3 Practical Implications

For Operators: The framework supports vendor selection (comparing proposals quantitatively), contract negotiation (risk scores inform SLA requirements), ongoing monitoring (periodic re-assessment per Blackhurst *et al.,* 2008), and compliance demonstration (systematic process for regulators per Jamison, 1999).

For Vendors: Understanding operator risk assessment enables targeted improvements. Security certifications' value is quantified (Higuero *et al.,* 2009; Tupa, 2012), guiding investment priorities.

For Regulators: The framework supports regulatory oversight of operator vendor risk management (Jamison, 1999) and provides foundation for industry standards, particularly for geopolitical risk (Moreno & Terwiesch, 2014).

For Other Industries: The adaptation template extends to critical infrastructure sectors (energy, finance, healthcare), demonstrating hybrid model value and transferable quantification methodology (Laeequddin *et al.,* 2013; Zhang *et al.,* 2006).

6.4 Comparison with Existing Approaches

Versus qualitative checklists (e.g., basic eTVRA), the framework adds quantification enabling prioritization (Higuero *et al.,* 2009), though requiring more complex weight elicitation. Versus pure financial models, comprehensive coverage beyond financial metrics addresses operational, security, and strategic risks (Zsidisin *et al.,* 2011), with trade-offs in data requirements. Versus single-standard approaches, the hybrid leverages complementary strengths (Tupa, 2012) despite integration complexity. Versus industry-specific models (automotive), telecommunications adaptations incorporate regulatory and geopolitical factors (Jamison, 1999; Moreno & Terwiesch, 2014) while sharing multi-criteria scoring approaches (Blackhurst *et al.,* 2008).

7. CONCLUSION

This research developed and validated the first COBIT-ISO hybrid framework for quantifying vendor risk in telecommunications. Through mixed-methods research combining expert panel validation (n=10) with AHP quantification applied to five vendors, the study demonstrates successful integration of COBIT governance, ISO 31000 risk management, and ISO 27001 security controls. The framework identifies five critical risk dimensions with 18 factors, achieving strong discriminant validity ($F=12.34$, $p<0.001$) and face

validity (ρ=0.89). Key contributions include extending IT governance theory to inter-organizational contexts, providing a hybrid framework integration template, advancing risk quantification methodology, and establishing telecommunications-specific vendor risk priorities. Practically, the framework provides operators with actionable assessment tools, vendors with improvement guidance, and regulators with oversight mechanisms.

Limitations include expert panel size (n=10), case sample size (n=5) limiting generalizability, cross-sectional design preventing longitudinal validation, AHP subjectivity, and context-specific development requiring adaptation for other regions or sectors. Future research should pursue longitudinal validation tracking risk scores against vendor outcomes, framework extensions incorporating network risk modeling and machine learning, broader applications to other industries and vendor types, integration with enterprise GRC systems, and comparative studies benchmarking effectiveness against alternative approaches. As telecommunications networks become increasingly critical and vendor ecosystems more complex, systematic vendor risk management is essential. This hybrid framework contributes theoretically by bridging governance and risk management literatures while providing practitioners with validated tools for vendor selection, monitoring, and portfolio management. The integration of COBIT, ISO 31000, and ISO 27001 demonstrates that combining complementary standards produces more comprehensive risk assessment than single-framework approaches, with quantification enabling the measurement rigor required for regulatory compliance and strategic decision-making in critical infrastructure contexts.

REFERENCES

- Blackhurst, J., Scheibe, K., & Johnson, D. (2008). Supplier risk assessment and monitoring for the automotive industry. International Journal of Physical Distribution & Logistics Management, 38(2), 143-165. https://doi.org/10.1108/09600030810875362
- Enyinda, C., Mbah, C., & Ogbuehi, A. (2013). An integrated fuzzy approach for aggregative supplier risk assessment. Journal of Manufacturing Technology Management, 24(4), 517-537. https://doi.org/10.1108/jmtm-06-2012-0066
- Higuero, M., Montalvo, J., Unzilla, J., & Jacob, E. (2009). Extended eTVRA vs. security checklist: Experiences in a value-web. Computers & Security, 28(1-2), 44-55. https://doi.org/10.1016/j.cose.2008.11.002
- Jamison, M. (1999). Mitigating regulatory risk in telecommunications. Public Utility Research Center, University of Florida.
- Laeequddin, M., Sardana, G., Sahay, B., Abdul Waheed, K., & Sahay, V. (2013). Elements of supplier risk assessment based on network AHP. International Journal of Procurement Management, 6(3), 316-334. https://doi.org/10.1504/ijpm.2013.050616
- Li, J., & Huang, S. (2010). Research on outsourcing risk evaluation and control. Proceedings of the International Conference on E-Business and E-Government, 5057-5060. https://doi.org/10.1109/icee.2010.1270
- Liu, S., & Wang, L. (2008). A study of the risks in an information system outsourcing partnership. International Seminar on Future BioMedical Information Engineering, 460-463. https://doi.org/10.1109/fbie.2008.100
- Luo, J. (2012). The vendor selection model of telecommunication operators based on dynamic fuzzy evaluation. Journal of Industrial Engineering and Management, 4, 20. https://doi.org/10.3969/j.issn.1003-7217.2012.04.020
- Moreno, A., & Terwiesch, C. (2014). Analysing supplier locations using social and semantic data: A case study in the telecommunication sector. Production and Operations Management, 23(4), 576-594. https://doi.org/10.1111/poms.12073
- Pletnev, D., & Nikolaeva, E. (2014). Risk management and sustainable development of telecommunications companies. Asian Social Science, 10(7), 10-19. https://doi.org/10.5539/ass.v10n7p10
- Rust, R., Lemon, K., & Zeithaml, V. (1996). Assessment of tools in the telecommunications industry: A customer perspective. International Journal of Service Industry Management, 7(5), 59-74. https://doi.org/10.1108/09564239610152536
- Swar, B., Moon, J., Oh, J., & Rhee, C. (2010). Managing risks in business critical outsourcing: A perspective from the telecommunication industry. International Journal of Business Research, 10(2), 156-172. https://doi.org/10.2139/ssrn.1653072
- Tupa, J. (2012). IT risk management framework based on ISO 31000:2009. In Risk Management for the Future (pp. 103-124). IntechOpen. https://doi.org/10.5772/50463
- Wu, D., & Olson, D. (2010). Enterprise risk management: A DEA VaR approach in vendor selection. International Journal of Production Research, 48(16), 4919-4932. https://doi.org/10.1080/00207540802635490
- Zhang, Z., Zhang, S., & Shi, Z. (2006). Partner assessment using MADM and ontology for telecom operators. Journal of Communication and Computer, 3(11), 232-237.
- Zsidisin, G., Hartley, J., Bernardes, E., & Saunders, L. (2011). A model for measuring supplier risk: Do operational capability indicators enhance financial risk predictions? International Journal of Physical Distribution & Logistics Management, 41(2), 1-21. https://doi.org/10.1108/ijpdlm.2011.08341baa.002