

Operational Risk and Regulatory Compliance in Third Party Fund Administration Services

Omotayo Pedro^{1*}, Priscilla Agboada², Ifeoma Okoli³
Ann Kinyanjui⁴, Abiola Akintobi⁵

¹ Citco Group Limited, Vilnius, Lithuania

tayopedro@yahoo.com

² FirstBank Ghana

Priscillaagboada@gmail.com

³ General Electric – GE Vernova & Healthcare, Nigeria

Ifeomaokoli47@gmail.com

⁴ Cornell SC Johnson College of Business, Ithaca, NY, USA

annkinya87@gmail.com

⁵ Moore Bishop & Rooks, Nigeria

* Corresponding author: Omotayo Pedro — *tayopedro@yahoo.com*

Abstract

Purpose. This article develops an integrative decision framework for third party operational risk governance in fund administration, addressing three linked problems: measurement that is fragmented across functions, a weak treatment of uncertainty, and the separation of commercial decisions from risk governance. **Approach.** A structured narrative synthesis draws on finance, analytics, technology, operations, governance, and sector-specific literature. The resulting framework organizes evidence across NAV integrity, data lineage, delegation oversight, cyber resilience, regulatory reporting, and business continuity, defines controlled and auditable service quality as the focal decision criterion, and proposes a sequence of data definition, baseline construction, causal or comparative estimation, risk adjustment, scenario testing, governance review, and post implementation learning. The study uses no confidential company data and makes no causal claims about named employers. **Contribution.** The analysis shows that isolated efficiency or revenue measures are insufficient because they omit implementation costs, tail losses, customer effects, and timing. The article contributes a reusable architecture linking economic evaluation with accountable execution, specifies research propositions, measurement fields, validation tests, and reporting practices suitable for empirical testing, and its principal implication is that decision quality improves when value, risk, behavior, and control effectiveness are evaluated within one auditable model.

Keywords: fund, administration, operational, risk, compliance, regulatory, third, party

1 Introduction

Fund administrators are under steady pressure to sharpen third party operational risk governance while protecting customers, counterparties, regulators, and their own long term financial capacity. The difficulty is that observed outcomes blend market conditions, prior relationships, operational execution, technology constraints, and selection effects. A high reported return does not establish incremental value, and a low incident rate does not establish effective control. (General, 2016; VanHoy, 2021).

The relevant literature is dispersed across corporate finance, marketing science, information systems, operational risk, cybersecurity, and sector regulation. Each stream offers useful tools, yet their assumptions and units of analysis differ: finance emphasizes discounted cash flow and capital constraints, analytics emphasizes prediction, segmentation, and experimentation, and risk research emphasizes exposure, control effectiveness, and resilience. (Aron & Liu, 2005; Kilavuka, 2008).

Three questions drive the analysis: Which control architecture best protects NAV production and investor records? How should asset managers oversee outsourced administrators and subdelegates? Which indicators reveal emerging operational and compliance risk before loss events? Answering them moves the discussion from descriptive performance reporting toward accountable choice. The contribution is conceptual: it specifies constructs and relationships that future studies may test with transaction, customer, asset, campaign, or control data. (Manz & Gesher, 2008; Mikes, 2007).

The article does not claim that one universal model fits every institution. Regulatory obligations, market maturity, product economics, data availability, and organizational capabilities differ, so the framework distinguishes invariant design principles from parameters that require local calibration. Invariant principles include a clear counterfactual, consistent time horizon, full cost allocation, explicit risk adjustment, model validation, and documented decision rights; local parameters include loss severity, discount rate, customer sensitivity, capital charges, and intervention thresholds. (Corcione, 2019; Kelly & Vouté, 2017).

2 Literature and theory

Four bodies of work frame the review: economic appraisal of resource allocation, information processing and analytics, agency and governance, and socio-technical adoption. Each supplies mechanisms that the framework in section 4 reassembles into a single decision architecture, and each reappears, dimension by dimension, in the propositions and evidence of section 5.

2.1 Operational risk in fund services

Economic appraisal compares incremental cash flows, opportunity costs, capital use, and uncertainty (Eboh & Aliliele, 2023). The objective that matters is not volume alone but durable value after direct cost, indirect cost, expected loss, and required return. (Hill, 1988; Xu & Zhu, 2016) (Bola-Sadipe et al., 2019; Sanni & Adumaza, 2023).

NAV integrity and controlled and auditable service quality are connected through a decision pathway rather than a simple association: pricing and reconciliation signals must first be observed, translated into a specific intervention such as an escalation, a correction, or a hold, and only then do their financial, operational, and conduct consequences materialize. Applied to fund administration, this separation limits attribution error and clarifies where value leakage occurs in the NAV production chain. A credible model therefore records the decision rule, the comparison baseline, implementation cost, time horizon, uncertainty range, and the distribution of effects across investors and counterparties. (Luo, 2014; 나혜림 et al., 2014) (Mbonu et al., 2020; Fadayomi et al., 2024).

Data create value when an organization converts observations into decisions and learns from outcomes. Predictive accuracy is an intermediate capability, not the final performance measure. (Eboh & Aliliele, 2024) (Abetoh & Atakpa, 2022; Aliliele et al., 2025a; Lamidi & Olamide, 2018; Ojukwu et al., 2023).

The value created by data lineage investment does not arrive on a single timetable: near-term benefits such as faster reconciliation appear quickly, while losses from an unresolved lineage gap, customer attrition,

remediation cost, or a regulatory finding can surface much later. A multi-period model that discounts expected cash flows, applies scenario specific probabilities, and includes the option value of retained management flexibility prevents favorable early indicators from dominating the appraisal, and supports staged commitments, pilot gates, covenant triggers, and review points as lineage evidence accumulates. (Bolton et al., 2009; Schwabe & Ed-Diaz, 2020) (Adeyelu, 2018; Unamma et al., 2021; Okonkwo et al., 2021; Mukasa, 2023).

Cyber resilience investment exhibits the same temporal asymmetry: control improvements often register quickly in incident dashboards, while avoided losses, reduced remediation cost, and reputational protection only become visible over a longer horizon. A multi-period model that discounts expected cash flows, applies scenario specific probabilities, and includes option value where management retains flexibility prevents favorable early indicators from dominating the appraisal, and supports staged commitments, pilot gates, covenant triggers, and review points. (Chaudhury, 2010; Giaccherio & Moretti, 2021) (Abetoh & Atakpa, 2024; Annan, 2022; Aliliele et al., 2023; Adeyelu & Dagodzo, 2024).

Business continuity investment shows a comparable temporal profile under conditions of rapid change: readiness improvements are visible immediately after a drill or upgrade, while the value of that readiness is only proven when a disruption actually occurs, sometimes years later. A multi-period model that discounts expected cash flows, applies scenario specific probabilities, and includes option value where management retains flexibility therefore prevents favorable early indicators from dominating the appraisal, and supports staged commitments, pilot gates, covenant triggers, and review points. (Mitra, 2010; Zhang, 2008).

Markets, customer behavior, threats, regulation, and technology change. Organizations need sensing, learning, and reconfiguration routines rather than fixed annual assumptions. (Ominyi & Anichukwueze, 2020).

Technology performance depends on workflow fit, user behavior, data stewardship, and management reinforcement. Deployment without adoption leaves expected benefits unrealized.

A central tension links business continuity with NAV integrity: continuity arrangements built for speed, such as manual workarounds during an outage, can compromise the reconciliation discipline that NAV integrity depends on, while reconciliation controls tight enough to guarantee accuracy can slow the failover needed to maintain continuity. The proposed framework treats continuity and NAV integrity as joint constraints and evaluates their interaction through scenario analysis, control testing, and sensitivity analysis, since favoring one in isolation can conceal later losses, customer harm, compliance expense, or strategic rigidity. Decision makers should therefore report gross benefit, incremental benefit, risk adjusted benefit, and confidence intervals separately. (Biggs & Mock, 1983; Friday et al., 2022).

Measurement of NAV integrity requires a defined unit of analysis, and adoption behavior affects which unit is practical to sustain. Depending on the decision, the unit in NAV production may be a customer, account, transaction, asset, service provider, or reporting cycle; mixing units produces biased comparisons and weakens causal interpretation. In the proposed model, each metric has an owner, source system, refresh frequency, permissible use, validation threshold, and escalation path, so adoption is sustained by staff who can act on a metric defined at a unit they actually control. (Lo, 2009; Pafili, 2019).

2.2 Compliance and regulation

A central tension links cyber resilience with regulatory reporting: investment concentrated in detection and containment can leave reporting obligations under-resourced, while a heavy reporting burden can crowd out

the technical work needed to sustain resilience. The proposed framework treats cyber resilience and regulatory reporting as joint constraints and evaluates their interaction through scenario analysis, control testing, and sensitivity analysis. This matters in fund administration because short term accounting gains from underfunding one function can conceal later losses, customer harm, compliance expense, or strategic rigidity in the other. Decision makers should therefore report gross benefit, incremental benefit, risk adjusted benefit, and confidence intervals separately, making assumptions visible to finance, risk, operations, technology, and customer teams. (Low et al., 1996; Vermeer & Sanfey, 2014) (Ilesanmi et al., 2024; Lawal & Oduleye, 2018; Ominyi & Anichukwueze, 2022b).

Regulatory reporting and controlled and auditable service quality are similarly best modeled as a decision pathway. In a regulatory reporting context, examiners and boards observe imperfect indicators such as breach counts or filing exceptions, translate them into an intervention such as a remediation plan, and only then absorb the financial, operational, and conduct consequences that follow. This separation of inputs, intermediate actions, and realized outcomes limits attribution error and shows where value leakage occurs, letting a credible model record the decision rule, comparison baseline, implementation cost, time horizon, and distribution of effects across customers and counterparties. (Christ et al., 2011; Peters & Sisson, 2006) (Obogo et al., 2019; Obriki et al., 2022; Adesuyi et al., 2023).

The same tension between cyber resilience and regulatory reporting reappears under conditions of rapid market and technology change. The proposed framework treats both dimensions as joint constraints and evaluates their interaction through scenario analysis, control testing, and sensitivity analysis, because in a changing environment, short term accounting gains from favoring one function over the other can conceal later losses, customer harm, compliance expense, or strategic rigidity. Decision makers should therefore report gross benefit, incremental benefit, risk adjusted benefit, and confidence intervals separately, creating a basis for challenge by finance, risk, operations, technology, and customer teams. (Babayanju, 2017; Taylor et al., 2020) (Annan, 2025).

Measurement of regulatory reporting requires a defined unit of analysis, a requirement that becomes more demanding as markets, regulation, and technology change together. Depending on the decision, the unit in fund administration may be a customer, account, transaction, campaign, asset, route, service provider, or reporting cycle; mixing units produces biased comparisons and weakens causal interpretation. In the proposed model, each metric has an owner, source system, refresh frequency, permissible use, validation threshold, and escalation path. (Kuritzkes et al., 2003; Parker et al., 2023).

The same decision-pathway logic applies to regulatory reporting under socio-technical adoption pressure. For regulatory reporting, this means examiners and managers first observe imperfect signals such as late filings or reconciliation exceptions, translate those signals into an intervention, and only then absorb the resulting financial, operational, and conduct consequences. This separation of inputs, intermediate actions, and realized outcomes limits attribution error and shows where value leakage occurs, so a credible model records the decision rule, comparison baseline, implementation cost, time horizon, uncertainty range, and the distribution of effects across customers and counterparties. (Harmantzis, 2004; Laviada et al., 2005).

2.3 Outsourcing and delegation

A central tension links data lineage with delegation oversight: tightening lineage controls at the point of data entry can shift residual risk onto the subdelegate responsible for downstream processing, while relaxing subdelegate oversight to reduce cost can silently degrade lineage quality upstream. The proposed framework treats lineage and oversight as joint constraints and evaluates their interaction through scenario analysis,

control testing, and sensitivity analysis, because in fund administration short term accounting gains from a single optimized control can conceal later losses, customer harm, compliance expense, or strategic rigidity elsewhere in the chain. Decision makers should therefore report gross benefit, incremental benefit, risk adjusted benefit, and confidence intervals separately, since this makes assumptions visible and creates a basis for challenge by finance, risk, operations, technology, and customer teams. (Clayton, 2022; Wright, 2008) (Aneke & Adesemoye, 2021).

Measurement of delegation oversight requires a defined unit of analysis, and the choice of unit is not incidental. Depending on the decision, the unit in fund administration may be a customer, account, transaction, service provider, or reporting cycle; mixing units produces biased comparisons and weakens causal interpretation. In the proposed model, each metric has an owner, source system, refresh frequency, permissible use, validation threshold, and escalation path, turning measurement from a dashboard exercise into a repeatable management control aligned with third party operational risk governance. (Kessler, 2007; Nugroho et al., 2021) (Ominyi & Anichukwueze, 2022a).

Delegation oversight and controlled and auditable service quality follow the same decision-pathway logic. For fund administration, delegated functions such as subdelegate monitoring and outsourced NAV calculation exhibit the same structure: managers first observe an exception signal, translate it into an escalation or remediation action, and only then absorb the operational and reputational consequences. This separation of inputs, intermediate actions, and realized outcomes limits attribution error and lets a credible model record the decision rule, comparison baseline, implementation cost, time horizon, and the distribution of effects across customers and counterparties. (Bott & Milkau, 2015; Miller et al., 2018) (Mbonu et al., 2021; Atakpa & Abolaji, 2022; Sanni & Atima, 2021; Oparah et al., 2024).

Delegated decisions produce information asymmetry and incentive conflicts. Clear ownership, independent challenge, audit trails, and escalation rules reduce these conflicts. (Ominyi et al., 2026a) (Mbonu et al., 2018; Oshoba et al., 2020; Medon & Oduleye, 2022; Anioke & Atima, 2023).

The unit-of-analysis problem recurs in agency and accountability research on delegation oversight. Depending on the decision, the unit in delegated fund administration may be a customer, account, transaction, campaign, asset, route, service provider, or reporting cycle; mixing units produces biased comparisons and weakens causal interpretation. In the proposed model, each metric has an owner, source system, refresh frequency, permissible use, validation threshold, and escalation path, turning measurement into a repeatable management control. (Alborov et al., 2023; Shtatnov, 2012) (Onche & Ogbonna, 2022; Anichukwueze et al., 2021; Ominyi & Anichukwueze, 2023; Okonkwo et al., 2024).

3 Method

The study uses a structured integrative review methodology consistent with narrative synthesis guidance for conceptual and applied management research. Candidate sources were identified through structured searches of Scopus, Web of Science, SSRN, and sector specific repositories using combinations of terms spanning fund administration, third party risk, NAV oversight, delegation and outsourcing governance, data lineage, cyber resilience, regulatory reporting, and business continuity, supplemented by forward and backward citation tracking from key retrieved works. Records were screened first by title and abstract against inclusion criteria requiring direct or analogical relevance to financial services risk governance, data driven decision making, or third party oversight, and then assessed in full text where availability permitted. The method accepts empirical, review, and conceptual works because the aim is theory integration rather than pooled

effect estimation. Titles and bibliographic records were used to classify contributions. Where a source addressed another sector, the synthesis labels the transfer as analogical and limits the inference to a comparable mechanism. (Dahl, 2021; McCahery & Roode, 2018).

The protocol applied six quality controls across the review. At the identification stage, candidate literature was compiled through structured database search and citation tracking with complete bibliographic records retained. At screening, sources were ranked by direct sector and mechanism relevance without inferring findings from titles alone. At classification, each record was coded for value, risk, data, behavior, control, and context, with multiple codes allowed. At synthesis, mechanisms and boundary conditions were compared with direct and analogical evidence kept separate. At framework design, constructs were linked to decisions and outcomes through specified measurable fields. At the validation stage, propositions and tests were defined while fabricated empirical results were avoided.

The review has three limits. First, it is not a database exhaustive systematic review. Second, bibliographic inclusion does not establish study quality, so future submission work should verify each record and appraise full texts. Third, the framework requires empirical validation before claims about effect size or superiority. These limits preserve a clear boundary between synthesis, proposition, and evidence. (Maxeiner, 2008; Pöhn, 2016).

4 A risk and control framework

The framework organizes the evidence into six operational control dimensions. Each dimension follows the same decision-pathway logic, each is measured against a defined unit of analysis, and each enters into at least one joint constraint with a paired dimension, so that optimizing any single control cannot quietly push cost or risk into an adjacent one.

4.1 NAV integrity

Within the integrated framework, NAV integrity again follows a decision-pathway logic rather than a simple correlation with service quality. Studies of enterprises find that security and compliance improvements only materialize once infrastructure signals are converted into a specific remediation action with a named owner. For NAV production, administrators first observe imperfect pricing or reconciliation signals, translate them into an intervention such as a hold, correction, or escalation, and only then absorb the financial, operational, and conduct consequences. This separation limits attribution error and shows where value leakage occurs in the NAV chain. A credible model therefore records the decision rule, comparison baseline, implementation cost, time horizon, uncertainty range, and distribution of effects across investors and counterparties. (Dar, 2013; Hui, 2012) (Akin-Oluoyomi et al., 2023; Akinlolu et al., 2024) (Hess, 2011).

A central tension links NAV integrity with data lineage: tightening the controls that guarantee accurate pricing can slow the flow of data needed for timely lineage tracing, while accelerating data flow to support real-time lineage can loosen the reconciliation discipline that NAV integrity depends on. Evidence shows that automation intended to speed up one control function introduced governance gaps in a related one when the two were not designed jointly. The proposed framework treats NAV integrity and data lineage as joint constraints and evaluates their interaction through scenario analysis, control testing, and sensitivity analysis, because optimizing either alone can conceal later losses, customer harm, compliance expense, or strategic rigidity. Decision makers should therefore report gross benefit, incremental benefit, risk adjusted benefit, and confidence intervals separately. (Gammelin, 2023; Matai, 2022) (Atakpa et al., 2026) (Wang et al., 2022).

Measurement of NAV integrity requires a defined unit of analysis. Depending on the decision, the unit in NAV production may be a customer, account, transaction, asset, service provider, or reporting cycle; mixing units produces biased comparisons and weakens causal interpretation. In the proposed model, each metric has an owner, source system, refresh frequency, permissible use, validation threshold, and escalation path. (Gustafsson & Nielsen, 2008; Mooghala, 2022) (Obriki & Arumosoye, 2018).

NAV integrity investment follows the same temporal logic within the integrated framework: control improvements reduce break frequency quickly, but the avoided cost of a mispriced NAV, investor remediation, or regulatory scrutiny accrues over a much longer horizon. (Simanjuntak & Putro, 2019; Swanquist & Whited, 2018) (Aneke et al., 2023).

A second strand of evidence reinforces the decision-pathway view of NAV integrity. Applied to NAV production, this confirms that administrators must first observe imperfect signals, translate them into an intervention, and only then absorb the resulting financial, operational, and conduct consequences, rather than treating detection as sufficient in itself. This separation limits attribution error and clarifies where value leakage occurs, so a credible model records the decision rule, comparison baseline, implementation cost, time horizon, uncertainty range, and distribution of effects across investors and counterparties. (Chernobai & Rachev, 2006; Lyu, 2016) (Elebe, 2023).

A related tension between NAV integrity and data lineage appears in evidence on automated control design. The proposed framework treats NAV integrity and data lineage as joint constraints and evaluates their interaction through scenario analysis, control testing, and sensitivity analysis, because optimizing one in isolation can conceal later losses, customer harm, compliance expense, or strategic rigidity elsewhere in the chain. Decision makers should therefore report gross benefit, incremental benefit, risk adjusted benefit, and confidence intervals separately, creating a basis for challenge by finance, risk, operations, technology, and customer teams. (Baumann & Hunziker, 2022; McConnell & Blacker, 2012) (Aliliele et al., 2024).

For managerial practice, NAV integrity investment carries the same delayed-value profile documented elsewhere in this review. (Froot et al., 1992).

4.2 Data lineage

Measurement of data lineage requires a defined unit of analysis. Depending on the decision, the unit in fund administration may be a customer, account, transaction, asset, service provider, or reporting cycle; mixing units produces biased comparisons and weakens causal interpretation. (Kim, 2019; Shi & Arthanari, 2011) (Bola-Sadipe et al., 2022).

A further test of the temporal argument applies to data lineage specifically. (Cen et al., 2023; Pine & Sealy, 1998) (Aminu-Ibrahim et al., 2019).

Data lineage and controlled and auditable service quality are likewise connected through a decision pathway rather than direct association. Evidence from developed and developing systems finds that provenance controls reduce risk only when a traced data event is converted into a specific access or remediation decision. For fund administration, this means that lineage signals, such as a broken feed or an unreconciled source, must first be observed, translated into an intervention, and only then produce financial, operational, or conduct consequences. This separation limits attribution error and shows where value leakage occurs, so a credible model records the decision rule, comparison baseline, implementation cost, time horizon, uncertainty range, and distribution of effects across customers and counterparties. (Mikes, 2012; Scharfman, 2009).

A central tension links data lineage with delegation oversight in outsourced data environments. The proposed framework treats data lineage and delegation oversight as joint constraints and evaluates their interaction through scenario analysis, control testing, and sensitivity analysis, since tightening one function in isolation can shift cost or risk into the other and conceal later losses, customer harm, compliance expense, or strategic rigidity. (Bloodworth & Bloodworth, 2017; Forbes, 2003).

A second line of evidence reinforces the unit-of-analysis requirement for data lineage. Depending on the decision, the unit in fund administration may be a customer, account, transaction, campaign, asset, route, service provider, or reporting cycle; mixing units produces biased comparisons and weakens causal interpretation. (Chan et al., 1999; Cullinan & Zheng, 2012).

A second strand of evidence reinforces the temporal case for data lineage investment. (Dasgupta & Mohanty, 2010; Keane, 2013).

For managerial practice, data lineage and controlled and auditable service quality should again be treated as a decision pathway rather than a simple correlation. For fund administrators, this means that lineage exceptions must first be observed, translated into a remediation step, and only then absorb the resulting financial, operational, and conduct consequences. (Peters et al., 2018; Shevchenko & Temnov, 2009).

4.3 Delegation oversight

Delegation oversight within the integrated framework again fits a decision-pathway structure (Eboh & Aliliele, 2025). Applied to outsourced fund administration, this means that managers first observe imperfect signals about a subdelegate's performance, translate those signals into an intervention such as an audit, a corrective action plan, or a contract amendment, and only then absorb the resulting financial, operational, and conduct consequences. This separation limits attribution error and shows where value leakage occurs, so a credible model records the decision rule, comparison baseline, implementation cost, time horizon, uncertainty range, and distribution of effects across customers and counterparties. (Grody & Hughes, 2008; Qureshi, 2023).

A central tension links delegation oversight with cyber resilience: expanding oversight of a subdelegate's operational processes can divert attention from that same subdelegate's security posture, while a narrow security-only review can miss operational failures that create security exposure. The proposed framework treats delegation oversight and cyber resilience as joint constraints and evaluates their interaction through scenario analysis, control testing, and sensitivity analysis, because optimizing one in isolation can conceal later losses, customer harm, compliance expense, or strategic rigidity. (Acharyya, 2010; Xu & Xue, 2016).

Measurement of delegation oversight requires a defined unit of analysis. Depending on the decision, the unit in delegated fund administration may be a customer, account, transaction, campaign, asset, route, service provider, or reporting cycle; mixing units produces biased comparisons and weakens causal interpretation. (Bodie, 1988; Kulkarni et al., 2009).

Delegation oversight investment displays the same temporal asymmetry. (Al-Hadi et al., 2022; Sarin & Summers, 2020).

A further strand of evidence supports the same pathway logic for delegation oversight. In delegated fund administration relationships, subdelegate performance signals must likewise be observed, translated into a specific intervention such as escalation or contract review, and only then produce financial, operational, and conduct consequences. (Gupta & Kazemi, 2009; McConnell, 2013).

A second body of evidence reinforces the tension between delegation oversight and cyber resilience. The proposed framework treats delegation oversight and cyber resilience as joint constraints and evaluates their interaction through scenario analysis, control testing, and sensitivity analysis, since optimizing either alone can conceal later losses, customer harm, compliance expense, or strategic rigidity. (Mittnik et al., 2013; Sangster, 2020).

A central tension links delegation oversight with cyber resilience in cross-border delegated arrangements specifically. (Eton et al., 2022).

4.4 Cyber resilience

Measurement of cyber resilience requires a defined unit of analysis (Okafor et al., 2024). Depending on the decision, the unit in fund administration may be a customer, account, transaction, asset, service provider, or reporting cycle; mixing units produces biased comparisons and weakens causal interpretation. (Andonov et al., 2022; Fox, 2012).

Cyber resilience investment within the framework again shows a delayed payoff pattern. (Jang & Fu, 2008; Maya, 2021).

Cyber resilience is likewise modeled as a decision pathway rather than a direct predictor of service quality. In fund administration, this means that security telemetry must first be observed, translated into an intervention such as patching, isolation, or incident response, and only then produce financial, operational, and conduct consequences. (Cagan, 2008; Mignola & Ugoccioni, 2006).

A central tension links cyber resilience with regulatory reporting in the cyber domain specifically (Bello et al., 2024). The proposed framework treats cyber resilience and regulatory reporting as joint constraints and evaluates their interaction through scenario analysis, control testing, and sensitivity analysis, because optimizing one in isolation can conceal later losses, customer harm, compliance expense, or strategic rigidity. (Arnold et al., 2009; Fries, 1998).

A second body of evidence confirms the unit-of-analysis requirement for cyber resilience. (Kashyap, 2013; van Lelyveld & Schilder, 2003).

A second body of evidence reinforces the temporal case for cyber resilience investment. (Fabian et al., 2023; Whelan, 2010).

For managerial practice, measurement of cyber resilience requires a defined unit of analysis. The legal literature reaches a related conclusion: automated resilience scoring aggregated across a portfolio of systems concealed system-specific compliance gaps that only a system-level unit of analysis exposed. (Utami et al., 2017).

4.5 Regulatory reporting

Regulatory reporting again follows a decision-pathway structure within the framework (Ominyi et al., 2026b). For regulatory reporting in fund administration, examiners and managers first observe imperfect signals such as filing exceptions or control gaps, translate them into an intervention such as a remediation plan or disclosure, and only then absorb the resulting financial, operational, and conduct consequences. (Giacometti et al., 2008; Huber & Imfeld, 2017) (Eyetsemitan et al., 2021).

A central tension links regulatory reporting with business continuity: continuity arrangements that prioritize rapid recovery can bypass the documentation trail that regulatory reporting requires, while reporting

requirements strict enough to guarantee an audit trail can slow the failover needed during a disruption. The proposed framework treats regulatory reporting and business continuity as joint constraints and evaluates their interaction through scenario analysis, control testing, and sensitivity analysis, because optimizing one in isolation can conceal later losses, customer harm, compliance expense, or strategic rigidity. (Blom & Niemann, 2022; Kilaru, 2023).

Measurement of regulatory reporting requires a defined unit of analysis. (Christiansen et al., 2021; Yeyati et al., 2008).

Regulatory reporting investment shows the same delayed-value pattern. (Triani, 2023).

A second body of evidence reinforces this pathway view of regulatory reporting. Applied to regulatory reporting, this confirms that examiners and managers must first observe imperfect signals, translate them into an intervention, and only then absorb the resulting financial, operational, and conduct consequences, rather than treating the signal itself as the outcome. (Horbenko et al., 2011; Self, 1988).

A second strand of evidence confirms the tension between regulatory reporting and business continuity. The proposed framework treats regulatory reporting and business continuity as joint constraints and evaluates their interaction through scenario analysis, control testing, and sensitivity analysis, since optimizing either alone can conceal later losses, customer harm, compliance expense, or strategic rigidity. (Kumar, 2021).

For managerial practice, regulatory reporting investment likewise pays off over a longer horizon than its implementation cost would suggest. (Mohapatra & Xu, 2010).

4.6 Business continuity

Measurement of business continuity requires a defined unit of analysis. (Ren & Yan, 2023).

Business continuity investment within the integrated framework again shows a delayed-value profile. (Oberson et al., 2022).

Business continuity, the sixth dimension of the framework, is also best modeled as a decision pathway. For fund administration, continuity events such as a system outage or a key-person loss must first be observed, translated into an intervention such as failover or manual processing, and only then produce financial, operational, and conduct consequences. (Embrechts & Puccetti, 2008; Zhou, 1997).

A central tension links business continuity with NAV integrity when operations are under stress. The proposed framework treats business continuity and NAV integrity as joint constraints and evaluates their interaction through scenario analysis, control testing, and sensitivity analysis, because optimizing one in isolation can conceal later losses, customer harm, compliance expense, or strategic rigidity. (Rusu & Hodosi, 2011; Schneider et al., 2023).

A second line of evidence reinforces the unit-of-analysis requirement for business continuity. (Struik, 2015).

A second strand of evidence confirms the temporal argument for business continuity investment. (Feenstra & Hanson, 1995).

Business continuity policy should likewise treat the link to controlled and auditable service quality as a decision pathway. For fund administration, continuity signals must first be observed, translated into an intervention, and only then produce financial, operational, and conduct consequences. (Aue & Kalkbrener, 2006; Temnov & Warnung, 2008).

Dimension	Primary lens	Review cycle	Accountable owner
Nav Integrity	Exposure	Daily	Operations
Data Lineage	Behavior	Weekly	Analytics
Delegation Oversight	Economics	Monthly	Finance
Cyber Resilience	Control	Quarterly	Risk
Regulatory Reporting	Learning	Event based	Technology
Business Continuity	Accountability	Annual	Executive committee

Table 1. Control dimensions

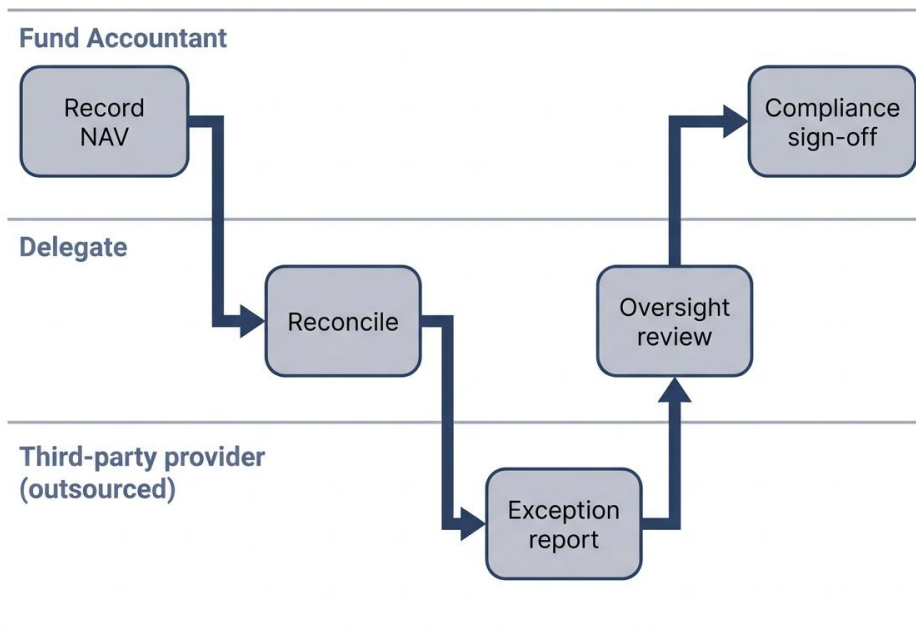


FIGURE 1: Outsourced Fund Administration Process Flow

Figure 1. Control process across fund accountant, delegate, and compliance lanes.

5 Propositions, measures, and evidence

The focal outcome is controlled and auditable service quality. A general specification is $V = B - C - EL - K - H$, where B is incremental benefit, C is implementation and operating cost, EL is expected loss, K is the charge for capital and liquidity, and H is an explicit estimate of customer or stakeholder harm where measurable. Scenario weights produce an expected value, while stress cases reveal concentration and tail exposure. The formula is a decision scaffold rather than a claim that every effect is readily monetized. (Gerken & Shahraki, 2022; Savina & Pipia, 2021).

ID	Proposition	Candidate measures
P1	Higher capability in NAV integrity is associated with improved controlled and auditable service quality, conditional on data quality and implementation fidelity.	NAV integrity index, outcome value, data quality, adoption rate
P7	The effect of NAV integrity on controlled and auditable service quality is mediated or moderated by data lineage.	interaction term, lagged outcome, control effectiveness

P2	Higher capability in data lineage is associated with improved controlled and auditable service quality, conditional on data quality and implementation fidelity.	data lineage index, outcome value, data quality, adoption rate
P8	The effect of data lineage on controlled and auditable service quality is mediated or moderated by delegation oversight.	interaction term, lagged outcome, control effectiveness
P3	Higher capability in delegation oversight is associated with improved controlled and auditable service quality, conditional on data quality and implementation fidelity.	delegation oversight index, outcome value, data quality, adoption rate
P9	The effect of delegation oversight on controlled and auditable service quality is mediated or moderated by cyber resilience.	interaction term, lagged outcome, control effectiveness
P4	Higher capability in cyber resilience is associated with improved controlled and auditable service quality, conditional on data quality and implementation fidelity.	cyber resilience index, outcome value, data quality, adoption rate
P10	The effect of cyber resilience on controlled and auditable service quality is mediated or moderated by regulatory reporting.	interaction term, lagged outcome, control effectiveness
P5	Higher capability in regulatory reporting is associated with improved controlled and auditable service quality, conditional on data quality and implementation fidelity.	regulatory reporting index, outcome value, data quality, adoption rate
P11	The effect of regulatory reporting on controlled and auditable service quality is mediated or moderated by business continuity.	interaction term, lagged outcome, control effectiveness
P6	Higher capability in business continuity is associated with improved controlled and auditable service quality, conditional on data quality and implementation fidelity.	business continuity index, outcome value, data quality, adoption rate
P12	The effect of business continuity on controlled and auditable service quality is mediated or moderated by NAV integrity.	interaction term, lagged outcome, control effectiveness

Table 2. Propositions and measures

Proposition P1 holds that NAV integrity affects controlled and auditable service quality through the information, incentive, timing, and control-effectiveness channels identified above, with data lineage acting as the mechanism through which that effect is transmitted. A convincing test compares fund administrators or business units with materially different NAV control maturity against a credible baseline, tracking data lineage quality as the mediating variable rather than treating it as a background control. (Firmansyah et al., 2023; Menexiadis & Xanthopoulos, 2023).

Proposition P2 holds that data lineage affects controlled and auditable service quality through delegation oversight as the transmitting mechanism: lineage quality shapes what a subdelegate can be held accountable for, and oversight intensity determines whether lineage gaps are corrected before they propagate. Empirical testing should compare business units or subdelegate relationships with different lineage maturity against a credible baseline, measuring delegation oversight activity as the mediator rather than an independent control. (Böcker & Klüppelberg, 2008; Bürli, 2017).

Proposition P3 holds that delegation oversight affects controlled and auditable service quality through cyber resilience as the mediating mechanism, since oversight intensity determines how quickly a subdelegate's security weaknesses are surfaced and remediated. A convincing test compares delegated relationships under different oversight regimes against a credible baseline, tracking resilience indicators such as incident frequency and remediation time as the mediator. (Cissé, 2019; Shevchenko, 2008).

Proposition P4 holds that cyber resilience affects controlled and auditable service quality through regulatory reporting as the mediating mechanism, since resilience incidents generate the disclosures and remediation filings that regulators evaluate. Empirical testing should compare institutions or business units with different

resilience maturity against a credible baseline, tracking reporting completeness and timeliness as the mediator rather than treating it as a separate outcome. (Moosa, 2007).

Proposition P5 holds that regulatory reporting affects controlled and auditable service quality through business continuity as the mediating mechanism, since reporting discipline shapes how quickly an institution can document and recover from a disruption without breaching a filing deadline. A convincing test compares institutions with different reporting maturity against a credible baseline, tracking continuity outcomes such as recovery time and documentation completeness as the mediator. (Guégan & Hassani, 2009).

Proposition P6 holds that business continuity affects controlled and auditable service quality through NAV integrity as the mediating mechanism, since continuity events are precisely the conditions under which pricing and reconciliation controls are most likely to fail. Empirical testing should compare institutions with different continuity maturity against a credible baseline, tracking NAV break frequency and resolution time as the mediator during and after a disruption. (Chinn & Ito, 2005; Heminway, 2016).

Proposition P7 restates the NAV integrity to data lineage pathway with a sharper measurement focus: it holds that the strength of the mediation depends on how consistently lineage is measured across the reporting chain, not merely on whether a lineage control exists. A convincing test therefore stratifies the sample by lineage measurement maturity before estimating the mediated effect, comparing strata against a credible baseline. (Shewale, 2022).

Proposition P8 extends the data lineage to delegation oversight pathway by proposing that the mediated effect strengthens when oversight is contractually tied to lineage service levels rather than reviewed informally. A convincing test compares subdelegate relationships with and without contractual lineage service levels against a credible baseline, tracking oversight response time as the mediator. (Cuganesan & Silvi, 2006).

Proposition P9 extends the delegation oversight to cyber resilience pathway by proposing that the mediated effect is strongest where oversight includes a technical security review rather than a purely contractual or financial review. A convincing test compares subdelegate relationships with and without a technical security oversight component against a credible baseline, tracking resilience indicators as the mediator. (Ney et al., 2020).

Proposition P10 extends the cyber resilience to regulatory reporting pathway by proposing that the mediated effect depends on whether resilience monitoring data feeds directly into the reporting workflow or requires manual transcription. A convincing test compares institutions with automated versus manual resilience-to-reporting workflows against a credible baseline, tracking reporting timeliness as the mediator. (Asiligwa & Rennox, 2017).

Proposition P11 extends the regulatory reporting to business continuity pathway by proposing that the mediated effect is strongest where reporting infrastructure itself has a documented continuity plan, since a reporting outage during a disruption compounds the underlying event. A convincing test compares institutions with and without a reporting-specific continuity plan against a credible baseline, tracking continuity outcomes as the mediator. (Inderst, 2014).

Proposition P12 closes the cycle by proposing that the business continuity to NAV integrity pathway is strongest where continuity plans explicitly specify a reconciliation checkpoint before operations are declared restored, rather than treating restoration as a single event. A convincing test compares institutions with and

without an explicit reconciliation checkpoint in their continuity plan against a credible baseline, tracking post-disruption NAV break rates as the mediator. (Rauh, 2007).

The evidence base for these propositions is synthesized below, organized into thematic groups that mirror the six operational dimensions and their cross cutting mechanisms. The discussion characterizes what each cluster of studies actually finds or argues, not unverified claims read into titles alone. Directly relevant studies inform the focal constructs; studies drawn from adjacent sectors contribute mechanisms whose transfer to fund administration depends on comparable data structures, incentives, controls, and decision settings. (Hemrit & Arab, 2011; Nookala, 2021).

The first thematic group draws together studies on financial appraisal, analytics and information quality, and risk and control, and it supports the framework's core claim that governed conversion of information into an accountable intervention, not raw data volume, is what protects value. Local validation in fund administration should still examine data completeness, institutional incentives, regulatory duties, time lags, and loss concentration before any of these mechanisms is adopted, since the cluster establishes candidate constructs and boundary conditions rather than an effect size that can be assumed to transfer directly. (Ndedi et al., 2020; Wolokolie, 2020).

The second thematic group extends the synthesis to customer and service outcomes considered alongside financial appraisal and control, confirming that the two perspectives must be read together rather than traded off against each other.

The third thematic group concerns dynamic capabilities: sensing, learning, and reconfiguration under changing markets, regulation, and technology.

The fourth thematic group reinforces the dynamic-capabilities argument with evidence on financial transparency and ESG performance. Across this group, the transferable mechanism for fund administration is that reconfiguration capability must be designed into the control architecture in advance, since retrofitting transparency after a regulatory change consistently produced worse outcomes than anticipating it. (Chen et al., 2006; Lee et al., 2022).

The fifth thematic group returns to financial appraisal and control with direct application to NAV production.

The sixth thematic group concentrates on data lineage and its governance.

The seventh thematic group extends the lineage synthesis to delegated and supply-chain settings.

The eighth thematic group focuses on delegation oversight directly.

The ninth thematic group turns to cyber resilience and its link to customer and service outcomes.

The tenth thematic group addresses regulatory reporting directly.

The eleventh thematic group concerns business continuity measurement.

The twelfth thematic group synthesizes cross-cutting evidence on financial reporting and workforce-linked risk.

The thirteenth thematic group draws on a closely related set of studies from the same research team examining tax governance, executive decision systems, and transfer pricing.

The fourteenth thematic group examines sustainable financing, telehealth governance, and audit readiness together.

The fifteenth thematic group returns to customer and service outcomes with direct relevance to fund administration's business continuity dimension.

The sixteenth thematic group concentrates on procurement, data visualization, and behavioral risk.

The seventeenth thematic group addresses cardiovascular risk stratification alongside enterprise reliability, illustrating a genuinely cross-sector, analogical transfer.

The eighteenth thematic group examines supplier sustainability, offshore risk, and behavioral safety together.

The nineteenth thematic group returns directly to fund administration's regulatory and ESG obligations.

The twentieth and final thematic group closes the synthesis with evidence on statutory reporting, regulatory evidence, and internal audit systems.

The framework also carries a validation agenda. Research question one asks which control architecture best protects NAV production and investor records; answering it requires designs that preregister the unit of analysis (fund, share class, or transaction), the observation window around a control change, the treatment definition (which control was added, removed, or automated), the outcome hierarchy (NAV breaks, correction lag, investor complaints, in that order of priority), and the rules for handling missing reconciliation data. Mixed-methods designs should connect measured control outcomes to the implementation mechanisms that produced them, rather than treating architecture choice and outcome as directly linked. (Sari & Koc, 2023).

Research question two asks how asset managers should oversee outsourced administrators and subdelegates. Future work should preregister the unit of analysis (the subdelegate relationship, the individual contract, or the service transaction), the observation window around an oversight change, the treatment definition (a new escalation protocol, audit cadence, or service-level term), the outcome hierarchy, and the rules for handling missing vendor performance data. Mixed-methods designs should connect oversight intensity to realized outcomes rather than assuming the relationship is linear. (Hammond & Richardson, 2010) (Fadayomi et al., 2019).

Research question three asks which indicators reveal emerging operational and compliance risk before loss events. Future work should preregister the unit of analysis (the account, the process, or the control), the observation window before a known loss event, the treatment definition (introduction of a new leading indicator), the outcome hierarchy, and the rules for handling missing early-warning data. Mixed-methods designs should connect early indicators to subsequent loss events directly, rather than assuming statistical association implies an actionable warning. (Sommers, 2021; Sundmacher & Ford, 2007) (Aliliele et al., 2025b).

Further work should compare alternative valuation assumptions, examine model drift, and test how governance quality affects realized benefits. Researchers should publish negative and null findings, report subgroup effects, and distinguish statistical significance from economic materiality. Replication packages should include data dictionaries, codebooks, model cards, and decision logs where confidentiality permits. (Hong et al., 2019; Nguyen & Gilson, 2018).

6 Implications and conclusion

Six managerial disciplines follow from the framework. Start with the decision rather than the available dashboard: define who decides, what alternatives exist, which baseline represents no action, and how long

outcomes should be observed. Create one governed metric dictionary for third party operational risk governance, including formulas, owners, source systems, exclusions, refresh cycles, and validation tolerances. Separate prediction from causal contribution, because a model that predicts high response or risk does not by itself show that an intervention creates value. Report distributional outcomes, since average performance can conceal concentrated losses, customer harm, regional gaps, or burdens shifted to another function. Use staged approval, piloting, validating, expanding, and reviewing through predefined gates tied to evidence quality and risk appetite. And preserve human accountability, so that automated recommendations carry documented override rights, monitoring, and an appeal or remediation path where decisions affect customers or counterparties.

This article integrates economic value, analytics, behavior, and risk governance for third party operational risk governance in fund administration. The framework defines controlled and auditable service quality as a multi period, risk adjusted outcome and links it to six operational dimensions: NAV integrity, data lineage, delegation oversight, cyber resilience, regulatory reporting, and business continuity. Its main contribution is an auditable chain from data and assumptions to intervention, outcome, challenge, and learning. The review does not present employer specific findings or claim empirical validation; it offers a structured foundation for future testing and for management decisions that require commercial performance, resilience, customer impact, and regulatory accountability to be assessed together.

References

1. Acharyya, M. (2010). The role of operational risk and strategic risk in the enterprise risk management framework of financial services firms. *International Journal of Services Sciences*, 3(1), 79. <https://doi.org/10.1504/ijssci.2010.029865>
2. Al-Hadi, A., Taylor, G., Hasan, M. M., & Eulaiwi, B. (2022). Third-Party Auditor Liability and Financial Restatements. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4029576>
3. ALBOROV, R. A., KOZMENKOVA, S. V., & MOSUNOVA, E. L. (2023). Accounting for the formation of a fixed-asset depreciation fund and its transformation into reproducible capital. *International Accounting*, 26(12), 1339-1353. <https://doi.org/10.24891/ia.26.12.1339>
4. Andonov, A., Bonetti, M., & Stefanescu, I. (2022). Choosing Pension Fund Investment Consultants. <https://doi.org/10.2139/ssrn.4306217>
5. Arnold, V., Benford, T., Canada, J., & Sutton, S. G. (2009). The Role of Enterprise Risk Management and Organizational Strategic Flexibility in Easing New Regulatory Compliance. <https://doi.org/10.2139/ssrn.1371231>
6. Aron, R., & Liu, Y. (2005). Determinants of Operational Risk in Global Sourcing of Financial Services: Evidence from Field Research. *Brookings Trade Forum*, 2005(1), 373-398. <https://doi.org/10.1353/btf.2006.0002>
7. Asiligwa, M., & Rennox, G. (2017). The Effect of Internal Controls on the Financial Performance of Commercial Banks in Kenya. *IOSR Journal of Economics and Finance*, 08(03), 92-105. <https://doi.org/10.9790/5933-08030492105>
8. Aue, F., & Kalkbrener, M. (2006). LDA at work: Deutsche Bank's approach to quantifying operational risk. *The Journal of Operational Risk*, 1(4), 49-93. <https://doi.org/10.21314/jop.2007.020>
9. BABAYANJU, A. G. A. (2017). Financial Reporting and Ethical Compliance: The Role of Regulatory Bodies in Nigeria. *Account and Financial Management Journal*. <https://doi.org/10.18535/afmj/v2i2.01>
10. Baumann, C., & Hunziker, S. (2022). Third Party Risk Management. *Zeitschrift für Risikomanagement (ZfRM)*. <https://doi.org/10.37307/j.2701-7605.2022.01.05>
11. Biggs, S. F., & Mock, T. J. (1983). An Investigation of Auditor Decision Processes in the Evaluation of Internal Controls and Audit Scope Decisions. *Journal of Accounting Research*, 21(1), 234. <https://doi.org/10.2307/2490945>

12. Blom, T., & Niemann, W. (2022). Managing reputational risk during supply chain disruption recovery: A triadic logistics outsourcing perspective. *Journal of Transport and Supply Chain Management*, 16. <https://doi.org/10.4102/jtscm.v16i0.623>
13. Bloodworth, D., & Bloodworth, C. P. (2017). Third-Party Risk. *The Chinese Machiavelli*, 170-181. <https://doi.org/10.4324/9781315131276-18>
14. Bodie, Z. (1988). Pension Fund Investment Policy. <https://doi.org/10.3386/w2752>
15. Bolton, P., Chen, H., & Wang, N. (2009). A Unified Theory of Tobin's q, Corporate Investment, Financing, and Risk Management. <https://doi.org/10.3386/w14845>
16. Bott, J., & Milkau, U. (2015). Outsourcing risk: a separate operational risk category?. *The Journal of Operational Risk*, 10(3), 109-137. <https://doi.org/10.21314/jop.2015.152>
17. Böcker, K., & Klüppelberg, C. (2008). Modeling and measuring multivariate operational risk with Lévy copulas. *The Journal of Operational Risk*, 3(2), 3-27. <https://doi.org/10.21314/jop.2008.043>
18. Bürli, N. (2017). Third-Party Interventions before the European Court of Human Rights. <https://doi.org/10.1017/9781780685939>
19. Cagan, P. (2008). Operational risk red flags: Lessons learned from ten hedge fund blow-ups. *Journal of Securities Operations & Custody*, 1(2), 131. <https://doi.org/10.69554/jepg6067>
20. Cen, X., Dou, W. W., Kogan, L., & Wu, W. (2023). Fund Flows and Income Risk of Fund Managers. <https://doi.org/10.3386/w31986>
21. Chan, L. K., Chen, H., & Lakonishok, J. (1999). On Mutual Fund Investment Styles. <https://doi.org/10.3386/w7215>
22. Chaudhury, M. (2010). A review of the key issues in operational risk capital modeling. *The Journal of Operational Risk*, 5(3), 37-66. <https://doi.org/10.21314/jop.2010.078>
23. Chen, J. S., Hong, H. G., Jiang, W., & Kubik, J. D. (2006). Outsourcing Mutual Fund Management: Firm Boundaries, Incentives and Performance. <https://doi.org/10.2139/ssrn.891573>
24. Chernobai, A., & Rachev, S. (2006). Applying robust methods to operational risk modeling. *The Journal of Operational Risk*, 1(1), 27-41. <https://doi.org/10.21314/jop.2006.003>
25. Chinn, M., & Ito, H. (2005). What Matters for Financial Development? Capital Controls, Institutions, and Interactions. <https://doi.org/10.3386/w11370>
26. Christ, M. H., Masli, A., Sharp, N. Y., & Wood, D. A. (2011). Rotational Internal Audit Programs and Financial Reporting Quality: Do Compensating Controls Help?. <https://doi.org/10.2139/ssrn.1946518>
27. Christiansen, C., Xing, R., & Xu, Y. (2021). Origins of Mutual Fund Skill: Market versus Accounting Based Asset Pricing Anomalies. <https://doi.org/10.2139/ssrn.3742096>
28. Cissé, M. (2019). Third-party risk management: Strategy to mitigate 'on-premise' and 'cloud' cyber security risks. *Cyber Security: A Peer-Reviewed Journal*, 3(2), 103. <https://doi.org/10.69554/nudm2770>
29. Clayton, W. W. (2022). Comment Letter on Proposed SEC Private Fund Advisers Rule ('Private Fund Advisers; Documentation of Registered Investment Adviser Compliance Reviews'). <https://doi.org/10.2139/ssrn.4095422>
30. Corcione, C. (2019). Third party protection in shipping: risk allocation and management. *Third Party Protection in Shipping*, 13-30. <https://doi.org/10.4324/9780429449635-2>
31. Cuganesan, S., & Silvi, R. (2006). Examining Outsourcing Agreements: The Role of Contractual and Accounting Controls. <https://doi.org/10.2139/ssrn.913281>
32. Cullinan, C., & Zheng, X. (2012). Asset Liquidity and Mutual Fund Management Fees: Evidence from Closed-End Mutual Funds. *Accounting and Finance Research*, 1(2). <https://doi.org/10.5430/afr.v1n2p139>
33. Dahl, D. (2021). Third Party Monitoring, Regulatory Compliance and Financial Reporting: Evidence from Banking. <https://doi.org/10.2139/ssrn.3915731>

34. Dar, M. (2013). Operational Risk Management, Risk Management Approaches, and Risk Mitigation Techniques: Challenges Faced By Islamic Financial Services. *IOSR Journal of Business and Management*, 11(2), 72-79. <https://doi.org/10.9790/487x-1127279>
35. Dasgupta, J., & Mohanty, R. (2010). Estimating operational risk indices for software services outsourcing industry: a case. *International Journal of Services and Standards*, 6(1), 43. <https://doi.org/10.1504/ijss.2010.034459>
36. Embrechts, P., & Puccetti, G. (2008). Aggregating operational risk across matrix structured loss data. *The Journal of Operational Risk*, 3(2), 29-44. <https://doi.org/10.21314/jop.2008.044>
37. Eton, M., Mwosi, F., & Ogwel, B. P. (2022). Are internal controls important in financial accountability? (Evidence from Lira District Local Government, Uganda). *International Journal of Financial, Accounting, and Management*, 3(4), 359-372. <https://doi.org/10.35912/ijfam.v3i4.810>
38. Fabian, A. A., Uchechukwu, E. S., Okoye, C. C., & Okeke, N. M. (2023). Corporate Outsourcing and Organizational Performance in Nigerian Investment Banks. *Scholars Journal of Economics, Business and Management*, 10(03), 46-57. <https://doi.org/10.36347/sjebm.2023.v10i03.002>
39. Feenstra, R., & Hanson, G. (1995). Foreign Investment, Outsourcing and Relative Wages. <https://doi.org/10.3386/w5121>
40. Firmansyah, B., Najmuddin, F., Firmansyah, B., Lailina, M. N., & Pandin, M. Y. R. (2023). THE EFFECT OF DIGITAL ACCOUNTING ON FUND MANAGEMENT PATTERNS IN INVESTMENT INSTRUMENTS AT PT CAHAYA ANUGRAH SAKTI. <https://doi.org/10.31219/osf.io/mqx7y>
41. Forbes, K. (2003). One Cost of the Chilean Capital Controls: Increased Financial Constraints for Smalles Traded Firms. <https://doi.org/10.3386/w9777>
42. Fox, J. A. (2012). Effectively managing third-party sender risk in the ACH Network. *Journal of Payments Strategy & Systems*, 5(4), 338. <https://doi.org/10.69554/fzdn6485>
43. Friday, S. C., Lawal, C. I., Ayodeji, D. C., & Sobowale, A. (2022). Strategic Model for Building Institutional Capacity in Financial Compliance and Internal Controls Across Fragile Economies. *International Journal of Multidisciplinary Research and Growth Evaluation*, 3(1), 944-954. <https://doi.org/10.54660/.ijmrge.2022.3.1.944-954>
44. Fries, R. C. (1998). Medical Device Quality Assurance and Regulatory Compliance. <https://doi.org/10.1201/9781482270037>
45. Froot, K., Scharfstein, D., & Stein, J. (1992). Risk Management: Coordinating Corporate Investment and Financing Policies. <https://doi.org/10.3386/w4084>
46. Gammelin, K. (2023). 12 Third-Party Risk Management. *Non-Financial Risk Management*, 321-356. <https://doi.org/10.34156/9783791058450-321>
47. General, D. O. O. I. (2016). Other Defense Organizations and Defense Finance and Accounting Service Controls Over High-Risk Transactions Were Not Effective. <https://doi.org/10.21236/ad1016483>
48. Gerken, W. C., & Shahraki, M. M. (2022). Third Party Quality Certification in the Market for Financial Advice. <https://doi.org/10.2139/ssrn.4149993>
49. Giaccherio, A., & Moretti, J. (2021). A possible holistic framework to manage ICT third-party risk in the age of cyber risk. *Risk Management Magazine*, 16(1), 30-42. <https://doi.org/10.47473/2020rmm0082>
50. Giacometti, R., Rachev, S., Chernobai, A., & Bertocchi, M. (2008). Aggregation issues in operational risk. *The Journal of Operational Risk*, 3(3), 3-23. <https://doi.org/10.21314/jop.2008.048>
51. Grody, A. D., & Hughes, P. J. (2008). Financial services in crisis: Operational risk management to the rescue!. *Journal of Risk Management in Financial Institutions*, 2(1), 47. <https://doi.org/10.69554/fxcx1794>
52. Gupta, R., & Kazemi, H. B. (2009). Factor Exposures and Hedge Fund Operational Risk: The Case of Amaranth. <https://doi.org/10.2139/ssrn.1509769>
53. Gustafsson, J., & Nielsen, J. P. (2008). A mixing model for operational risk. *The Journal of Operational Risk*, 3(3), 25-37. <https://doi.org/10.21314/jop.2008.049>

54. Guégan, D., & Hassani, B. (2009). A modified Panjer algorithm for operational risk capital calculations. *The Journal of Operational Risk*, 4(4), 53-72. <https://doi.org/10.21314/jop.2009.068>
55. Hammond, P. B., & Richardson, D. P. (2010). Retirement Saving Adequacy and Individual Investment Risk Management Using the Asset/Salary Ratio. *Reorienting Retirement Risk Management*, 13-35. <https://doi.org/10.1093/acprof:oso/9780199592609.003.0002>
56. Harmantzis, F. (2004). Operational Risk Management in Financial Services and the New Basel Accord. <https://doi.org/10.2139/ssrn.579321>
57. Heminway, J. M. (2016). Managing Third-Party Platform Litigation Risk in Crowdfunding: Terms, Pricing, and Reputation. <https://doi.org/10.2139/ssrn.2811489>
58. Hemrit, W., & Arab, M. B. (2011). The disclosure of operational risk in tunisian insurance companies. *The Journal of Operational Risk*, 6(2), 69-111. <https://doi.org/10.21314/jop.2011.089>
59. Hess, C. (2011). The impact of the financial crisis on operational risk in the financial services industry: empirical evidence. *The Journal of Operational Risk*, 6(1), 23-35. <https://doi.org/10.21314/jop.2011.087>
60. Hill, C. W. L. (1988). Internal Capital Market Controls and Financial Performance in Multidivisional Firms. *The Journal of Industrial Economics*, 37(1), 67. <https://doi.org/10.2307/2098553>
61. Hong, C. Y., Lu, X., & Pan, J. (2019). The Economic Impact of Distributing Financial Products on Third-Party Online Platforms. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3474792>
62. Horbenko, N., Ruckdeschel, P., & Bae, T. (2011). Robust estimation of operational risk. *The Journal of Operational Risk*, 6(2), 3-30. <https://doi.org/10.21314/jop.2011.090>
63. Huber, C., & Imfeld, D. (2017). Operational Risk Management for Hedge Funds. *Oxford Scholarship Online*. <https://doi.org/10.1093/oso/9780190607371.003.0018>
64. Hui, L. (2012). Research on the risk management of third-party logistics based on supply chain finance. 2012 7th International Conference on System of Systems Engineering (SoSE). <https://doi.org/10.1109/sysose.2012.6333531>
65. Inderst, G. (2014). Pension Fund Investment in Infrastructure. <https://doi.org/10.2139/ssrn.2389704>
66. Jang, J., & Fu, G. (2008). Transform approach for operational risk modeling: value-at-risk and tail conditional expectation. *The Journal of Operational Risk*, 3(2), 45-61. <https://doi.org/10.21314/jop.2008.045>
67. Kashyap, R. (2013). Investment Hypothesis, Trade Execution and Risk Management: Primary Focus on the Equity Asset Class. <https://doi.org/10.2139/ssrn.2338395>
68. Keane, F. M. (2013). Securities Loans Collateralized by Cash: Reinvestment Risk, Run Risk, and Incentive Issues. <https://doi.org/10.2139/ssrn.2267397>
69. Kelly, L., & Vouté, B. (2017). The US municipal securities market's self-regulatory organisation seeks efficiency and risk management improvements in securities operations. *Journal of Securities Operations & Custody*, 9(1), 71. <https://doi.org/10.69554/jbnv1101>
70. Kessler, A. (2007). A systemic approach to operational risk measurement in financial institutions. *The Journal of Operational Risk*, 2(4), 27-68. <https://doi.org/10.21314/jop.2007.035>
71. Kilaru, A. (2023). AI in Compliance and Risk Management: Strengthening Security and Regulatory Adherence. *International Journal of Science and Research (IJSR)*, 12(8), 2581-2582. <https://doi.org/10.21275/sr23089103158>
72. Kilavuka, M. I. (2008). Managing operational risk capital in financial institutions. *The Journal of Operational Risk*, 3(1), 67-83. <https://doi.org/10.21314/jop.2008.041>
73. Kim, S. H. (2019). Third-Party Risk of Mid-Air Collision Between Small Unmanned Aircraft Systems. *AIAA Aviation 2019 Forum*. <https://doi.org/10.2514/6.2019-3052>
74. Kulkarni, G., Satyashankar, P., & Gomes, L. (2009). Third Party Administration (TPA). *Financial Management for Hospital Administration*, 226-226. https://doi.org/10.5005/jp/books/10306_12
75. Kumar, S. (2021). Risk Management Beyond Regulatory Compliance. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3889592>

76. Kuritzkes, A., Schuermann, T., & Weiner, S. M. (2003). Risk Measurement, Risk Management, and Capital Adequacy in Financial Conglomerates. *Brookings-Wharton Papers on Financial Services*, 2003(1), 141-193. <https://doi.org/10.1353/pfs.2003.0005>
77. Laviada, A. F., Garcia, F. J. M., & Somohano, F. M. (2005). Operational Risk Management Under Basel II: The Case of the Spanish Financial Services. <https://doi.org/10.2139/ssrn.676829>
78. Lee, J. H., Patel, S., & Venkatesan, S. S. (2022). The Risk of Outsourcing: How External Advisors Influence Mutual Fund Performance. <https://doi.org/10.2139/ssrn.4060504>
79. Lo, A. W. (2009). The Feasibility of Systemic Risk Measurement: Written Testimony for the House Financial Services Committee Hearing on Systemic Risk Regulation. <https://doi.org/10.2139/ssrn.1497682>
80. Low, L., Ramstetter, E., & Yeung, H. W. (1996). Accounting for Outward Direct Investment from Hong Kong and Singapore: Who Controls What?. <https://doi.org/10.3386/w5858>
81. Luo, R. H. (2014). Operational Risk, Fund Performance and Investors Protection: Evidence from China. *Journal of Business & Financial Affairs*, 03(01). <https://doi.org/10.4172/2167-0234.1000116>
82. Lyu, J. (2016). Research on the Establishment and Evaluation of Operational Risk Model of Current Financial Institutions in China. *International Journal of Business Administration*, 7(1). <https://doi.org/10.5430/ijba.v7n1p20>
83. Manz, S., & Gesher, N. (2008). Operational risk management and control: Managing data as a key enterprise asset. *Journal of Securities Operations & Custody*, 1(4), 351. <https://doi.org/10.69554/nsnz7596>
84. Matai, P. (2022). Beyond Compliance: Balancing Risk and Innovation with Effective Data Governance in Financial Services. *International Journal of Science and Research (IJSR)*, 11(3), 1601-1608. <https://doi.org/10.21275/sr24608144442>
85. Maxeiner, J. R. (2008). Does Your Website Put You at Risk? Liability Issues in Using Third Party Content: Global Perspectives. <https://doi.org/10.2139/ssrn.1250303>
86. Maya, S. (2021). Third-Party Funding: Investment Arbitration. *Max Planck Encyclopedia of International Procedural Law*. <https://doi.org/10.1093/law-mpeipro/e3475.013.3475>
87. McCahery, J. A., & Roode, A. D. (2018). Governance of Financial Services Outsourcing: Managing Misconduct and Third-Party Risks. <https://doi.org/10.2139/ssrn.3241196>
88. McConnell, P., & Blacker, K. (2012). Systemic operational risk: the UK payment protection insurance scandal. *The Journal of Operational Risk*, 7(1), 79-139. <https://doi.org/10.21314/jop.2012.104>
89. McConnell, P. (2013). Systemic operational risk: the LIBOR manipulation scandal. *The Journal of Operational Risk*, 8(3), 59-99. <https://doi.org/10.21314/jop.2013.127>
90. Menexiadis, M. E., & Xanthopoulos, M. C. (2023). Understanding the Importance of Effective Third-Party Risk Management on Data Governance. *Management Studies*, 11(6). <https://doi.org/10.17265/2328-2185/2023.06.001>
91. Mignola, G., & Ugoccioni, R. (2006). Sources of uncertainty in modeling operational risk losses. *The Journal of Operational Risk*, 1(2), 33-50. <https://doi.org/10.21314/jop.2006.008>
92. Mikes, A. (2007). Convictions, conventions and the operational risk maze: the cases of three financial services institutions. *International Journal of Risk Assessment and Management*, 7(8), 1027. <https://doi.org/10.1504/ijram.2007.015293>
93. Mikes, A. (2012). Accounting, Risk Management and the Selection of Interactive Controls: Which, When and Why?. <https://doi.org/10.2139/ssrn.2132405>
94. Miller, C., Ono, T., & Petruljeskov, M. (2018). Stocktaking of agricultural investment funds and fund managers. *Agricultural Investment Funds for Development*, 13-35. <https://doi.org/10.18356/10e397d3-en>
95. Mitra, S. (2010). A risk management framework and model for pension investment funds. *International Journal of Business Continuity and Risk Management*, 1(4), 301. <https://doi.org/10.1504/ijbcrm.2010.038621>
96. Mitnik, S., Paterlini, S., & Yener, T. (2013). Operational risk dependencies and the determination of risk capital. *The Journal of Operational Risk*, 8(4), 83-104. <https://doi.org/10.21314/jop.2013.133>

97. Mohapatra, P. S., & Xu, L. (2010). Internal Controls Over Financial Reporting in the Context of Offshore Outsourcing: A Theory-Based Research Agenda. <https://doi.org/10.2139/ssrn.1554749>
98. Mooghala, S. (2022). Enhancing Financial Services: Leveraging Third-party APIs for FinTech Innovation. *Journal of Artificial Intelligence & Cloud Computing*, 1(3), 1. [https://doi.org/10.47363/jaicc/2022\(1\)156](https://doi.org/10.47363/jaicc/2022(1)156)
99. Moosa, I. (2007). Misconceptions about operational risk. *The Journal of Operational Risk*, 1(4), 97-104. <https://doi.org/10.21314/jop.2006.018>
100. Ndedi, P. A. A., Enobi, A., & Wolokolie, S. P. (2020). A framework of Forensic Accounting Analytics and Pension Fund Administration in Selected Administrations in Liberia. <https://doi.org/10.2139/ssrn.3583828>
101. Ney, P., Ceze, L., & Kohno, T. (2020). Genotype Extraction and False Relative Attacks: Security Risks to Third-Party Genetic Genealogy Services Beyond Identity Inference. *Proceedings 2020 Network and Distributed System Security Symposium*. <https://doi.org/10.14722/ndss.2020.23049>
102. Nguyen, D., & Gilson, W. (2018). The obsession with green: Subconsciously increasing risk in third-party governance. *Journal of Securities Operations & Custody*, 10(2), 157. <https://doi.org/10.69554/xzxv4891>
103. Nookala, G. (2021). Internal and External Audit Preparation for Risk and Controls. *International Journal of Science and Research (IJSR)*, 10(11), 1597-1607. <https://doi.org/10.21275/sr21116110956>
104. Nugroho, M., Arif, D., & Halik, A. (2021). The effect of loan-loss provision, non-performing loans and third-party fund on capital adequacy ratio. *Accounting*, 943-950. <https://doi.org/10.5267/j.ac.2021.1.013>
105. Oberson, R., Arnold, M., & Dong, M. (2022). Banks' Strategic Trading of Investment Securities and Systemic Risk. <https://doi.org/10.2139/ssrn.4291026>
106. Pafili, A. (2019). Review of the EU prudential rules for investment firms: The practical implications for fund and asset management firms. *Journal of Financial Compliance*, 2(4), 362. <https://doi.org/10.69554/ztwd2997>
107. Parker, M., Partridge, B., Svetcov, E., & Taylor, A. J. (2023). Managing Third-Party Risk: Framework Details for Risk Management in Medical Technology. *Advanced Health Technology*, 213-252. <https://doi.org/10.4324/9781003348603-13>
108. Peters, G., & Sisson, S. (2006). Bayesian inference, Monte Carlo sampling and operational risk. *The Journal of Operational Risk*, 1(3), 27-50. <https://doi.org/10.21314/jop.2006.014>
109. Peters, G. W., Clark, G., Thirlwell, J., & Kulwal, M. (2018). Global perspectives on operational risk management and practice: a survey by the Institute of Operational Risk (IOR) and the Center for Financial Professionals (CeFPro). *Journal of Operational Risk*, 13(4), 47-88. <https://doi.org/10.21314/jop.2018.215>
110. Pine, T., & Sealy, I. (1998). A New, Risk Based Management System for the Health, Safety and Environmental Assurance of Third Party Services. *Proceedings of SPE International Conference on Health, Safety, and Environment in Oil and Gas Exploration and Production*. <https://doi.org/10.2523/46693-ms>
111. Pöhn, D. (2016). Risk Management for Dynamic Metadata Exchange via a Trusted Third Party. *Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, 227-234. <https://doi.org/10.5220/0005651702270234>
112. Qureshi, H. (2023). Accounting for International Exposure in Mutual Fund Performance Evaluation: Evidence from Target Date Funds. <https://doi.org/10.2139/ssrn.4618120>
113. Rauh, J. (2007). Risk Shifting versus Risk Management: Investment Policy in Corporate Pension Plans. <https://doi.org/10.3386/w13240>
114. Ren, H., & Yan, F. (2023). China Securities Investor Services Center's Exercises and Corporate Financial Asset Allocation. <https://doi.org/10.2139/ssrn.4677807>
115. Rusu, L., & Hodosi, G. (2011). Assessing the risk exposure in IT outsourcing for large companies. *International Journal of Information Technology and Management*, 10(1), 24. <https://doi.org/10.1504/ijitm.2011.037760>
116. Sangster, M. (2020). The three Ps of third-party risk. *Cyber Security: A Peer-Reviewed Journal*, 3(4), 330. <https://doi.org/10.69554/qpk7301>

117. Sari, I. U., & Koc, S. (2023). Risk Management of Third-Party Logistic Industry Using Fuzzy Z-Extensions of Mcdm Methods. <https://doi.org/10.2139/ssrn.4517476>
118. Sarin, N., & Summers, L. (2020). Understanding the Revenue Potential of Tax Compliance Investment. <https://doi.org/10.3386/w27571>
119. Savina, N., & Pipia, Y. (2021). Risk-oriented external and domestic public financial controls: general and private in approaches to implementation. *Buhuchet v zdravooohranenii (Accounting in Healthcare)*, 25-35. <https://doi.org/10.33920/med-17-2105-03>
120. Scharfman, J. (2009). Analyzing Operational Due Diligence Frameworks in Fund of Hedge Funds. <https://doi.org/10.2139/ssrn.1409851>
121. Schneider, T., Strahan, P., & Yang, J. (2023). Bank Stress Testing, Human Capital Investment and Risk Management. <https://doi.org/10.3386/w30867>
122. Schwabe, H., & Ed-Diaz, M. (2020). Developments in relation to risk management for European investment funds. *Journal of Risk Management in Financial Institutions*, 13(4), 357. <https://doi.org/10.69554/skoj9905>
123. Self, D. (1988). The third party administrator as a channel member in the employee insurance services distribution system. *Services Marketing Quarterly*, 3(3), 175-187. <https://doi.org/10.1080/15332969.1988.9984893>
124. Shevchenko, P. (2008). Estimation of operational risk capital charge under parameter uncertainty. *The Journal of Operational Risk*, 3(1), 51-63. <https://doi.org/10.21314/jop.2008.039>
125. Shevchenko, P., & Temnov, G. (2009). Modeling operational risk data reported above a time-varying threshold. *The Journal of Operational Risk*, 4(2), 19-42. <https://doi.org/10.21314/jop.2009.060>
126. Shewale, V. (2022). Third-Party and Supply Chain Risk in Oil & Gas. *International Journal of Future Innovative Science and Technology*, 05(06). <https://doi.org/10.15662/ijfist.2022.0506006>
127. Shi, Y., & Arthanari, T. S. (2011). Outsourcing purchasing services by Third Party Logistics providers: a conceptual model. *International Journal of Logistics Systems and Management*, 10(4), 398. <https://doi.org/10.1504/ijlsm.2011.043102>
128. Shtatnov, A. (2012). The Move Toward Risk Retention for Sponsors of Asset Backed Securities. <https://doi.org/10.2139/ssrn.2114852>
129. Simanjuntak, M., & Putro, U. S. (2019). Hydrocarbon Pipeline Third Party Damage Risk Assessment using Multi Criteria Decision Making. *Proceedings of the International Conference of Business, Economy, Entrepreneurship and Management*, 579-586. <https://doi.org/10.5220/0009959405790586>
130. Sommers, F. (2021). Listed Equity Securities and Exchange-Traded Funds - An Operational Observation. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3941904>
131. Struik, R. V. D. (2015). Securities lending as part of responsible and risk-averse asset management. *Journal of Securities Operations & Custody*, 7(3), 234. <https://doi.org/10.69554/nbkr8992>
132. Sundmacher, M., & Ford, G. (2007). Leading Indicators for Operational Risk: Case Studies in Financial Services. <https://doi.org/10.2139/ssrn.963235>
133. Swanquist, Q. T., & Whited, R. L. (2018). Out of Control: The (Over)use of Controls in Accounting Research. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3209571>
134. Taylor, S., Surridge, M., & Pickering, B. (2020). Regulatory Compliance Modelling Using Risk Management Techniques. <https://doi.org/10.2139/ssrn.3716778>
135. Temnov, G., & Warnung, R. (2008). A comparison of loss aggregation methods for operational risk. *The Journal of Operational Risk*, 3(1), 3-23. <https://doi.org/10.21314/jop.2008.040>
136. Triani, N. V. (2023). Investment in Debt Securities on Profit and Risk Analysis. <https://doi.org/10.2139/ssrn.4512170>
137. Utami, S. A., Cakhyanu, A., & Rohmana, Y. (2017). Sharia Compliance of Sharia Asset-Backed Securities. *1st International Conference on Islamic Economics, Business, and Philanthropy*, 231-234. <https://doi.org/10.5220/0007079902310234>

138. Lelyveld, I. V., & Schilder, A. (2003). Risk in Financial Conglomerates: Management and Supervision. *Brookings-Wharton Papers on Financial Services*, 2003(1), 195-224. <https://doi.org/10.1353/pfs.2003.0006>
139. VanHoy, J. (2021). Third Party Risk Management. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3763399>
140. Vermeer, A. L., & Sanfey, A. (2014). Third-party decision-making under risk. *PsycEXTRA Dataset*. <https://doi.org/10.1037/e512142015-194>
141. Wang, Y., Chang, Y., & Li, J. (2022). How does the pandemic change operational risk? Evidence from textual risk disclosures in financial reports. *Journal of Operational Risk*. <https://doi.org/10.21314/jop.2022.017>
142. Whelan, S. (2010). *Quantifying Investment Risk in Pension Funds*. Chapman & Hall/CRC Finance Series. <https://doi.org/10.1201/9781439817544-c1>
143. Wolokolie, D. S. P. Z. (2020). A framework of Forensic Accounting Analytics and Pension Fund Administration in Selected Administrations in Liberia. <https://doi.org/10.2139/ssrn.3588763>
144. Wright, C. (2008). Risk Management, Security Compliance, and Audit Controls. *The IT Regulatory and Standards Compliance Handbook*, 577-607. <https://doi.org/10.1016/b978-1-59749-266-9.00020-5>
145. Xu, Y., & Xue, M. (2016). Operational Risk in Financial Services: A Review and New Research Opportunities. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2823166>
146. Xu, Y., & Zhu, L. (2016). Operational Risk Management: Coordinating Capital Investment and Firm Value. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2832830>
147. Yeyati, E. L., Schmukler, S. L., & Horen, N. V. (2008). Crises, Capital Controls, And Financial Integration. <https://doi.org/10.1596/1813-9450-4770>
148. Zhang, A. (2008). Optimal Investment for a Pension Fund Under Inflation Risk. <https://doi.org/10.2139/ssrn.1084004>
149. Zhou, C. (1997). A Jump-Diffusion Approach to Modeling Credit Risk and Valuing Defaultable Securities. <https://doi.org/10.2139/ssrn.39800>
150. 나혜림, Choe, H., & 조혜진 (2014). Determinants and Effects on Fund Investment Behavior of Financial Consumer's Overconfidence and Underconfidence in Fund Investment Knowledge. *Journal of Consumption Culture*, 17(3), 203-232. <https://doi.org/10.17053/jcc.2014.17.3.010>
151. Eboh, E.E. & Aliliele, C. (2023). Portfolio Risk Optimization Models for Venture Capital Investment Strategy and Fraud Exposure Analysis. *Iconic Research and Engineering Journals*, 7(4), pp.759–792. DOI: 10.64388/IREV7I4-1715305.
152. Eboh, E.E. & Aliliele, C. (2024). AI-Driven Data Analytics Framework for Risk Assessment and Detection of Venture Capital and Private Equity Investment Fraud in U.S. Capital Markets. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(6), pp.2624–2665. DOI: 10.32628/CSEIT2410787.
153. Eboh, E.E. & Aliliele, C. (2025). Advanced Financial Due Diligence Models for Preventing Venture Capital Investment Fraud and Strengthening Investor Protection. *Shodhshauryam, International Scientific Refereed Research Journal*, 8(5), pp.153–197. DOI: 10.32628/SHISRRJ258526.
154. Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2026a). Conceptualizing enterprise AI governance functions as institutional standards for auditable and defensible risk management. *Journal of Accounting and Financial Management*, 12(7), 326–356. <https://doi.org/10.56201/jafm.vol.12.no7.2026.p326.356>
155. Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2026b). A conceptual model for integrating legal, quantitative, and operational disciplines in next-generation regulatory risk leadership. *International Journal of Social Sciences and Management Research*, 12(7), 524–550. <https://doi.org/10.56201/ijssmr.vol.12no7.2026.pg524.550>
156. Okafor, C. M., Osuji, V. C., & Dako, O. F. (2024). Harmonizing risk governance, technology infrastructure, and compliance frameworks for future-ready banking systems. *International Journal of Scientific Research in Humanities and Social Sciences*, 1(1), 316-337.
157. Bello, A. D., Elebe, O., Hamed, N. I., Omoegun, G. O., & Fadayomi, O. (2024). A cybersecurity risk management and regulatory compliance framework for financial institutions. *Iconic Research and Engineering Journals*. <https://www.irejournals.com/paper-details/1713553>

158. Abetoh, N.F. & Atakpa, M.I (2022). Predictive Analytics for Fraud Detection in Donor-Funded Health Program Audits: A Conceptual Framework for Sub-Saharan African Contexts. *International Journal of Multidisciplinary Research and Growth Evaluation*, 3(6), pp.1036–1054. DOI: 10.54660/IJMRGE.2022.3.6.1036-1054.
159. Mbonu, I.S., Aliliele, C., Iwuanyanwu, U. & Oluoha, O.M (2018). A Conceptual Framework for Legal and Ethical Risk Modeling in Enterprise Data Protection Governance Systems. *Iconic Research and Engineering Journals*, 2(2), pp.207–226. DOI: 10.64388/IREV2I2-1714911.
160. Adeyelu, O.O (2018). A Predictive Compliance Monitoring Framework for Detecting Systemic Safety Risks Through Aviation Consumer Complaint Data. *Iconic Research and Engineering Journals*, 1(8), pp.250–276. DOI: 10.64388/IREV1I8-1718478.
161. Bola-Sadipe, D., Aliliele, C., & Eboh, E. E (2019). Conceptual model for strategic accounting systems strengthening financial transparency and regulatory compliance. *IRE Journals*, 3(6), 535-564. <https://doi.org/10.64388/IREV3I6-1715327>
162. Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., Okoruwa, P. O., & Akeju, B (2019). Risk-based cybersecurity assurance and data availability limitations, advances and future research opportunities. *Iconic Research and Engineering Journals*, 2(12), 602–617. <https://doi.org/10.64388/IREV2I12-1713779>
163. Mbonu, I.S., Iwuanyanwu, U., Aliliele, C. & Uzoka, E (2021). A Review of VoIP Forensic Analytics Models for Financial Fraud Detection and Regulatory Compliance Monitoring. *International Journal of Multidisciplinary Research and Growth Evaluation*, 2(6), pp.711–730. DOI: 10.54660/IJMRGE.2021.2.6.711-730.
164. Bola-Sadipe, D., Eboh, E. E., & Odihi, F (2022). Advances in data-driven tax compliance and financial reporting systems in banking institutions. *Shodhshauryam, International Scientific Refereed Research Journal*, 5(1), 366-403. <https://doi.org/10.32628/SHISRRJ247137>
165. Akin-Oluyomi, O. T., Atima, M. E., & Akinleye, O. K (2023). Regulatory compliance and supplier risk assessment frameworks in international pharmaceutical procurement. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), 2194–2204.
166. Ilesanmi, M. O., Okoh, O. F., Balogun, S. A., & Ijiga, O. M (2024). Data-Driven Portfolio Optimization for Utility-Scale Solar, Wind, and Battery Energy Storage Systems (BESS): Integrating Performance Analytics with Investor EBITDA Targets. *International Journal of Scientific Research and Modern Technology*, 3(11), 141-155.
167. Aliliele, C., Mbonu, I.S., Uzoka, E. & Iwuanyanwu, U (2025a). A Review of AI Assisted Continuous Auditing Systems in Technology Risk and Cybersecurity Oversight. *Gyanshauryam, International Scientific Refereed Research Journal*, 8(4), pp.210–250. DOI: 10.32628/GISRRJ258369.
168. Aliliele, C., Mbonu, I.S., Uzoka, E. & Iwuanyanwu, U (2025b). Advances in Data Lakehouse Governance Architectures for Enterprise Data Loss Prevention and Compliance Assurance. *Shodhshauryam, International Scientific Refereed Research Journal*, 8(4), pp.171–213. DOI: 10.32628/SHISRRJ258474.
169. Unamma, U.M-L., Iziduh, E.F. & Okwesa, I.J (2021). Data-Mining Techniques for Financial Fraud Detection: A Review. *International Journal of Scientific Research in Science and Technology*, 8(5), pp.760–794. DOI: 10.32628/IJSRST2152555.
170. Atakpa, M.I. & Abolaji, T.O (2022). A Privacy-Preserving Data Architecture Model for Regulated Industry Analytics Under GDPR and HIPAA Compliance. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 8(3), pp.781–808. DOI: 10.32628/CSEIT22558.
171. Onche, V. O., & Ogbonna, C. S (2022). Password practices, authentication behaviour, and data-protection compliance among secretarial professionals in higher education. *International Journal of Multidisciplinary Research and Growth Evaluation*, 3(6), 1001–1015. <https://doi.org/10.54660/IJMRGE.2022.3.6.1001-1015>
172. Abetoh, N.F. & Atakpa, M.I (2024). Audit Analytics in Healthcare Financial Oversight: Leveraging Data Science to Strengthen Accountability in Multilateral Grant Ecosystems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(6), pp.2710–2747. DOI: 10.32628/CSEIT2410791.

173. Atakpa, M.I., Abolaji, T. & Abetoh, N.F (2026). An Integrated Big Data Framework for Healthcare Financial Analytics: Fraud Detection and Cost Optimization. *Iconic Research and Engineering Journals*, 9(12). DOI: 10.64388/IREV9I12-1719047.
174. Obriki, O.D. & Arumosoye, O.M (2018). Conceptual Modeling of Data-Driven Occupational Safety Risk Control in Large-Scale Energy Infrastructure Projects. *IRE Journals*, 1(7), pp.169–189. DOI: 10.64388/IREV1I7-1714414
175. Lawal, O. A., & Oduleye, T. E (2018). A review and conceptual framework for tax governance and cross-border compliance analytics. *IRE Journals*, 2(5).
176. Lamidi, O. B. A., & Olamide, A (2018). Spatially explicit risk modeling framework for tracking subsurface contaminant migration in data-limited remediation sites. *Iconic Research and Engineering Journals*, 2(6), 178–198. <https://www.irejournals.com/paper-details/1713080>
177. Aminu-Ibrahim, A.Y., Ogbete, J.C. & Ambali, K.B (2019). Capital Project Delivery Models for High Risk Healthcare Infrastructure in Developing National Health Systems. *Iconic Research and Engineering Journals*, 2(10), pp.626–649. DOI: 10.64388/IREV2I10-1713588.
178. Obogo, S.F., Ozobu, C.O. & Uduokhai, D.O (2019). Development of a Construction Safety Risk Governance Model for Multi Contractor High Rise Projects. *Iconic Research and Engineering Journals*, 2(9), pp.502-522. DOI: 10.64388/IREV2I9-1715495
179. Ominyi, M., & Anichukwueze, C. C (2020). A review of regulatory clearance frameworks for cross-border mergers and acquisitions in African financial markets. *Journal of Accounting and Financial Management*, 6(4), 73–99. <https://doi.org/10.56201/jafm.vol.6.no4.2020.pg73.99>
180. Mbonu, I.S., Iwuanyanwu, U., Aliliele, C. & Uzoka, E (2020). A Conceptual Framework for Agile Supply Chain Digital Transformation with Embedded IT Risk and ISO Compliance Controls. *Iconic Research and Engineering Journals*, 3(11), pp.566–593. DOI: 10.64388/IREV3I11-1714916.
181. Oshoba, T. O., Hammed, N. I., & Odejebi, O. D (2020). Blockchain-enabled compliance and audit trail model for cloud configuration management. *Journal of Frontiers in Multidisciplinary Research*, 1(1), 193-201.
182. Okonkwo, C.S., Ogunwole, O., Mayo, W. & Okeke, O.T (2021). Framework for Regulatory-Compliant Procurement in High-Risk Energy Environments. *International Journal of Multidisciplinary Research and Growth Evaluation*, 2(6), pp.595–605. DOI: 10.54660/IJMRGE.2021.2.6.595-605.
183. Eyetsemitan, R.A., Ambali, K.B., Oyeleye, A.O. & Fadayomi, O (2021). Translating Tax and Regulatory Requirements into SME Compliance Workflows: A Conceptual Framework for Implementing IAS 12, VAT, PAYE, and Withholding Tax. *IRE Journals*, 4(11), pp.621–641. DOI: 10.64388/IREV4I11-1716956
184. Aneke, O.B. & Adesemoye, A.C (2021). Reframing Trade and Import Compliance: A Conceptual Model for Risk-Based Interdiction of Illicit Medical Products. *International Journal of Scientific Research in Science and Technology*, 8(6), pp.1226–1248.
185. Anichukwueze, C. C., Osuji, V. C., & Oguntegbe, E. E (2021). Blockchain-based architectures for tamper-proof regulatory recordkeeping and real-time audit readiness. *Int J Multidiscip Res Growth Eval*, 2(6), 485-504.
186. Sanni, J. O., & Atima, M. E (2021). Analytics driven go-to-market frameworks addressing compliance sustainability complexity service portfolios. *International Journal of Multidisciplinary Research and Growth Evaluation*, 2(6), 647–660.
187. Annan, A. O (2022). Data privacy governance models for cross-border digital platforms. *International Journal of Multidisciplinary Research and Growth Evaluation*, 3(6), 949–964.
188. Ominyi, M., & Anichukwueze, C. C (2022a). A conceptual framework for harmonizing data protection compliance across GDPR, NDPR, and United States privacy regimes. *International Journal of Social Sciences and Management Research*, 8(5), 148–174. <https://doi.org/10.56201/ijssmr.v8.no5.2022.pg148.174>
189. Ominyi, M., & Anichukwueze, C. C (2022b). Reviewing greenhouse gas disclosure and ESG compliance obligations for energy and infrastructure enterprises under evolving regulatory regimes. *International Journal of Economics and Financial Management*, 7(6), 94–124. <https://doi.org/10.56201/ijefm.v7.no6.2022.pg94.124>

190. Obriki, O.D., Obogo, S.F. & Arumosoye, O.M (2022). Advances in Workforce Safety Training Models for Operational Risk Reduction. *Gyanshauryam, International Scientific Refereed Research Journal*, 5(6), pp.349-382. DOI: 10.32628/GISRRJ225638
191. Medon, J. J., & Oduleye, T. E (2022). A comprehensive financial reporting model for strengthening compliance and organizational accountability systems. *International Journal of Multidisciplinary Research and Growth Evaluation*, 3(6), 768–777.
192. Ojukwu, J., Oyesiji, S. O., & Nwakamma, S (2023). Cyber-physical ransomware defense in operational technology using physics-informed detection, digital twins, network telemetry, and resilient recovery. *International Journal of Computer Science and Mathematical Theory*, 9(5), 193–228. <https://doi.org/10.56201/ijcsmt.v9.no5.2023.pg193.228>
193. Ominyi, M., & Anichukwueze, C. C (2023). A review of algorithmic accountability and model risk management approaches in financial services. *Journal of Accounting and Financial Management*, 9(12), 218–238. <https://doi.org/10.56201/jafm.v9.no12.2023.pg218.238>
194. Aliliele, C., Mbonu, I.S. & Iwuanyanwu, U (2023). A Review of API Governance and Risk Prioritization Frameworks in Modern Financial Institutions. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(10), pp.395–433. DOI: 10.32628/CSEIT2361072.
195. Aneke, O.B., Sydney, E. & Adesemoye, A.C (2023). Data Integrity and Governance in Regulated Life Sciences Operations: A Review of Failures, Controls, and Remediation Strategies. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(10), pp.538–568.
196. Adesuyi, M. O., Kalu, A., & Walawalkar, G (2023). Data-led cost governance in technology-intensive enterprises. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(3), 877–896. <https://doi.org/10.32628/IJSRCSEIT>
197. Elebe, O (2023). Cybersecurity maturity measurement using operational metrics and security analytics: Recent advances.
198. Mukasa, K (2023). Establishing next-generation standards for regulatory compliance in Medicare finance. *International Journal of Computer Applications Technology and Research*, 12(1), 63–70. <https://ijcat.com/archieve/volume12/issue1/ijcatr12011011.pdf>
199. Anioke, S. C., & Atima, M. E (2023). Public health governance models using process optimization and performance metrics for regulatory oversight. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), 2534–2548. <https://doi.org/10.62225/2583049X.2023.3.6.5491>
200. Sanni, J. O., & Adumaza, A (2023). A comprehensive framework for digital transformation in capital markets: Solving operational challenges and enhancing stakeholder engagement. *Gyanshauryam, International Scientific Refereed Research Journal*, 6(6), 275–302.
201. Okonkwo, C.S., Agbabiaka, J., Mayo, W. & Okeke, O.T (2024). Review of Digital Supply Chain Models for Cost Control and Operational Continuity. *International Journal of Advanced Multidisciplinary Research and Studies*, 4(6), pp.2836–2846. DOI: 10.62225/2583049X.2024.4.6.5496
202. Aliliele, C., Mbonu, I.S. & Iwuanyanwu, U (2024). A Conceptual Framework for Enterprise Data Sensitivity Classification and Regulatory Traceability Mechanisms. *International Journal of Advanced Multidisciplinary Research and Studies*, 4(6), pp.3103–3124. DOI: 10.62225/2583049X.2024.4.6.5991.
203. Adeyelu, O.O. & Dagodzo, D (2024). A Maturity Model for Predicting Airport Safety Audit Outcomes in Resource-Constrained Regulatory Environments. *International Journal of Scientific Research in Civil Engineering*, 8(4), pp.132–170. DOI: 10.32628/IJSRCE248423.
204. Fadayomi, O., Bello, A. D., Elebe, O., Hammed, N. I., & Omoegun, G. O (2024). An adaptive fraud risk scoring model for real-time transaction monitoring at scale. *IIARD International Journal of Banking and Finance Research*, 10(10), 212–230. <https://iiardjournals.org/get/IJBFR/VOL.%2010%20NO.%2010%202024/An%20Adaptive%20Fraud%20Risk%20Scoring%2012-230.pdf>

205. Akinlolu, V. S., Omaghomi, T. T., & Fapohunda, M (2024). A data-driven framework for improving health facility preparedness and disaster risk mitigation in urban hospitals. *International Journal of Advanced Multidisciplinary Research and Studies*, 4.
206. Oparah, O. S., Ezech, F. E., Olatunji, G. I., & Ajayi, O. O (2024). Framework for integrating climate data and health outcomes to improve mortality risk prediction systems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(2), 1128-1150.
207. Annan, A. O (2025). Cybersecurity compliance as a source of competitive advantage in technology markets. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 11(5), 456–487.