© NOV 2018 | IRE Journals | Volume 2 Issue 5 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV2I5-1722619

IT Governance Frameworks (COBIT/ITIL) and Their Impact on Regulatory Compliance in Nigerian Insurance Firms

SAMUEL FADERO[1]*, SERIF OYINDAMOLA OYESIJI[2], STANLEY NWAKAMMA[3], DEMILADE JOODA[4]

[1]*SanlamAllianz Life Insurance Ltd, Lagos Nigeria*
[2]*Independent Researcher, Lagos Nigeria*
[3]*Independent Researcher, USA*
[4]*Fasyl Technology Ghana - Accra, Ghana*
**Corresponding Author: Samuel Fadero*

Abstract- ***This review examines how structured information technology governance and service-management practices can strengthen regulatory compliance, operational resilience, and digital accountability within Nigerian insurance firms. Its purpose is to evaluate the complementary roles of COBIT and ITIL, assess their relevance to technology-related regulatory obligations, and identify implementation conditions capable of improving governance maturity across the sector. A structured narrative review method was adopted, drawing on peer-reviewed scholarship, recognised governance frameworks, and relevant regulatory and professional literature published up to 2018. The analysis synthesised evidence on governance structures, internal controls, service management, cybersecurity, risk oversight, auditability, digital transformation, and compliance monitoring.***

The findings show that COBIT provides a robust architecture for strategic alignment, control ownership, risk optimisation, performance evaluation, and assurance, while ITIL strengthens operational reliability through incident, change, availability, continuity, and service-level management. Their integration offers a coherent governance-to-operations model through which regulatory expectations can be translated into measurable and auditable technology practices. However, implementation effectiveness is constrained by uneven governance maturity, legacy systems, skills shortages, infrastructure limitations, fragmented accountability, cybersecurity exposure, and the cost of sustained process improvement. The review concludes that successful adoption requires contextual tailoring rather than mechanical framework implementation.

It recommends phased, risk-based COBIT–ITIL integration, stronger board and executive oversight, clearer control ownership, enhanced cybersecurity capability, continuous service-performance monitoring, and closer alignment between technology governance, internal audit, enterprise risk management, and regulatory reporting. Future research should empirically test how governance maturity influences compliance outcomes, service reliability, audit findings, operational performance, and regulatory costs within Nigerian insurance firms. Such evidence can support proportionate regulation and sustainable sector-wide digital resilience.

Keywords: COBIT; ITIL; IT governance; regulatory compliance; Nigerian insurance; digital governance.

I. INTRODUCTION

1.1 Evolution of IT Governance in Insurance

The evolution of IT governance in insurance reflects the industry's transition from viewing information technology as a back-office utility to recognising it as a strategic, risk-bearing and value-creating corporate resource. Early insurance systems were principally designed to automate policy administration, premium accounting, actuarial calculations and claims processing. As databases, networks and enterprise applications became embedded in underwriting and customer service, technology decisions increasingly affected operational continuity, financial control and corporate performance. Research on governance implementation subsequently demonstrated that organisations achieve stronger business–IT alignment when structures, relational mechanisms and decision processes are combined rather than treated as isolated technical controls (De Haes & Van Grembergen, 2009).

This shift was particularly significant for insurers because their business models depend upon information quality, risk classification, contractual accuracy and sustained access to customer records. Governance therefore developed beyond the management of hardware and software toward the allocation of decision rights, accountability for technology investments and executive oversight of information-related risks. Evidence from Canada showed that board competence, organisational characteristics and the strategic role of IT influence the degree of board involvement in technology governance, reinforcing the movement of IT oversight into corporate governance structures (Jewer & McKay, 2012). In South Africa, however, research on IT projects found uneven adherence to established governance principles, illustrating that formal frameworks do not automatically translate into disciplined organisational practice (Marnewick & Labuschagne, 2011).

Within Nigeria, the insurance industry's technological evolution similarly created a need for stronger managerial capability around IT resources. Empirical evidence from Nigerian insurers indicated that IT investment alone was insufficient to secure superior customer-service outcomes; performance improved when technological resources interacted with firm-specific managerial capabilities (Aduloju, 2014). This finding is important to the evolution of governance thinking because it moves attention from technology acquisition toward stewardship, capability development and strategic control. Nigerian technical research outside insurance also demonstrated the growing sophistication of automated analytical systems through computer-aided mammographic detection using template-matching techniques; although not an insurance-governance study, it provides limited contextual evidence of the wider expansion of algorithmic decision-support technologies that increased the importance of governance over automated information processing (Ejofodomi et al., 2014).

Internationally, the governance agenda also became associated with measurable organisational value. Evidence from Brazilian firms found that organisations adopting IT-governance mechanisms experienced improved financial performance relative to a control group, particularly after governance practices had time to become institutionalised (Lunardi et al., 2014). This strengthened the rationale for insurers to treat governance not merely as a compliance expense but as an architecture for extracting value from technology while constraining operational and strategic risk.

The maturation of frameworks such as COBIT further formalised this transition. Empirical investigation of COBIT 5 showed that governance and management processes were positively associated with achievement of IT-related and enterprise goals, while also revealing that governance maturity declines where stronger business and board participation is required (De Haes et al., 2016). Governance consequently evolved toward enterprise-wide responsibility rather than exclusive ownership by IT departments. This development is particularly pertinent to insurance firms, where technology decisions intersect with underwriting controls, solvency management, customer protection, privacy, auditing and regulatory reporting.

By the late 2010s, governance frameworks were increasingly connected to internal-control architecture. Analysis of COBIT demonstrated that structured IT-governance processes can strengthen control-environment assessment by linking responsibilities, processes and assurance mechanisms, thereby making technology governance more relevant to auditability and regulatory discipline (Rubino et al., 2017). Simultaneously, digitalisation was transforming the insurance value chain through data-intensive underwriting, automated processes, connected platforms and changing customer interfaces. These developments altered information asymmetries and introduced new dependencies created by technological connectivity, making governance central to both value creation and risk containment (Eling & Lehmann, 2018).

Accordingly, the historical trajectory of IT governance in insurance can be understood as a progressive expansion of scope: from operational systems control, to business–IT alignment, to board-level accountability, enterprise risk oversight and digitally enabled regulatory assurance. For Nigerian insurance firms, this evolution is especially consequential

because digital transformation intensifies dependence on reliable information systems while exposing weaknesses in governance maturity, managerial capability and control integration. Modern IT governance therefore represents an institutional mechanism through which insurers can align technology with corporate objectives, clarify accountability, preserve information integrity and prepare their digital operations for increasingly rigorous compliance expectations.

1.2 Regulatory Compliance and Technology Risks in Nigerian Insurance

Regulatory compliance in Nigerian insurance has become increasingly intertwined with technology risk as insurers digitise underwriting, claims, customer administration and financial reporting. The environment is shaped by institutional conditions where formal governance rules coexist with enforcement and accountability challenges. Adegbite (2012) argues that Nigerian corporate-governance regulation is strongly conditioned by local institutional realities, implying that insurance firms cannot treat compliance as a mechanical exercise in rule adoption. For technology-dependent insurers, effective compliance requires governance arrangements that translate regulatory obligations into accountable information-system controls and auditable decision processes.

The risk profile becomes more complex as insurers accumulate personal and financial information. South African experience demonstrates that cybersecurity governance requires coordinated legal, institutional and organisational responses rather than isolated technical safeguards, where privacy and data protection intersect (Sutherland, 2017). This perspective is pertinent to Nigerian insurers because digital service delivery enlarges exposure to unauthorised access, service interruption, data leakage, third-party vulnerabilities and weaknesses in incident response, potentially undermining regulatory assurance and policyholder confidence.

Cyber risk is difficult to govern because historical loss information is limited, threat conditions change rapidly, and losses may be correlated across organisations. Empirical analysis identifies obstacles involving information asymmetry, accumulation risk and insufficient data, creating challenges for risk assessment and insurability (Biener, Eling & Wirfs, 2015). Within insurance operations, these characteristics make cybersecurity controls relevant to operational resilience, underwriting discipline and regulatory risk management.

The international literature further shows that cyber risk combines technological, behavioural, legal and economic dimensions, meaning conventional risk-management structures may inadequately capture its evolving characteristics (Eling & Schnell, 2016). Nigerian insurers consequently require compliance architectures linking information security, enterprise risk management, internal control and service continuity rather than assigning cyber exposure solely to technical departments.

Evidence from United States property and casualty insurers indicates that corporate recognition of cyber risk increased as digital threats became more salient, demonstrating how technology risk entered insurers' formal risk disclosures and strategic concerns (Pooser, Browne & Arkhangelska, 2018). Such recognition is important for Nigerian firms facing expanding digital dependencies and expectations concerning reliable records and controlled information processing.

Regulatory compliance increasingly extends beyond avoiding sanctions toward demonstrating appropriate organisational behaviour around data protection. Cyber insurers can influence compliance by promoting security assessments, breach-response practices and privacy-oriented controls among insured organisations (Talesh, 2018). This illustrates a broader governance imperative for Nigerian insurers: technology risks must be identified, controlled, documented and connected to regulatory accountability across the insurance value chain.

1.3 COBIT and ITIL for Governance and Service Management

COBIT and ITIL occupy complementary positions within contemporary information technology governance and service management. COBIT provides an enterprise-oriented structure for directing, controlling and evaluating information and technology, while ITIL concentrates on the disciplined design, transition, operation and continual

improvement of IT-enabled services. Their combined relevance to insurance arises from the sector's dependence on reliable information systems, auditable processes and uninterrupted service delivery. Research on IT governance implementation indicates that successful governance depends not merely on adopting formal controls, but on organisational commitment, clear responsibilities, communication, skills and alignment between business and technology priorities (Alreemy et al., 2016).

ITIL operationalises this governance intent by structuring repeatable service-management practices around incidents, changes, availability, capacity and service continuity. Cross-national evidence shows that ITIL adoption is widespread but uneven, with organisations tending to implement operational processes more extensively than tactical and strategic practices, suggesting that maturity requires progression beyond technical support toward integrated managerial oversight (Marrone et al., 2014). For regulated insurers, such progression is important because service failures can disrupt underwriting, claims administration, customer records and regulatory reporting.

The relationship between COBIT and ITIL is therefore better understood as complementary rather than substitutive. Systematic analysis of both frameworks demonstrates that COBIT supplies governance objectives, control expectations and performance oversight, whereas ITIL offers more detailed service-management processes through which governance requirements can be embedded in daily operations (Veronica & Suryawan, 2017). In the African context, information assets are increasingly recognised as organisational resources requiring coherent control, protection and lifecycle management; service-management frameworks such as ITIL consequently contribute to the capability required to safeguard these assets and sustain their value (Adesemowo, Von Solms & Botha, 2016).

This interaction is particularly pertinent to Nigerian insurance firms. Empirical evidence from Nigeria shows that effective use of information technology can improve service delivery and organisational performance in insurance, while also requiring regular evaluation of IT utilisation and stronger managerial attention to technology-enabled services (Idris, Olumoko & Ajemunigbohun, 2013). Applied together, COBIT and ITIL can provide Nigerian insurers with a governance-to-service architecture linking strategic oversight, accountability and control with dependable operational execution, and regulatory assurance.

1.4 Aim, Scope, Objectives, and Review Method

This review aims to critically examine the role of IT governance frameworks, particularly COBIT and ITIL, in strengthening regulatory compliance within Nigerian insurance firms. It focuses on how governance structures, service-management practices, internal controls, risk oversight, and technology-enabled processes can support insurers in meeting regulatory, operational, cybersecurity, and data-governance obligations. The scope covers the interaction between enterprise IT governance and service management, with particular attention to control effectiveness, accountability, auditability, incident management, business continuity, information security, and regulatory reporting within the Nigerian insurance environment.

The review pursues four principal objectives: to evaluate the conceptual foundations of COBIT and ITIL; to assess their relevance to regulatory compliance and technology-risk management; to examine the potential benefits and implementation constraints associated with their adoption in Nigerian insurance organisations; and to identify emerging governance priorities capable of improving compliance maturity and operational resilience. Particular emphasis is placed on the complementary use of COBIT for governance, control, and performance oversight, and ITIL for structured service delivery and continual improvement.

Methodologically, the study adopts a structured narrative review of peer-reviewed literature, recognised governance frameworks, professional standards, and relevant regulatory materials. Sources are critically synthesised to compare theoretical perspectives, empirical findings, and practical applications, while highlighting contextual gaps specific to Nigeria. This approach supports a balanced assessment of existing knowledge and identifies areas requiring further empirical investigation.

II. FOUNDATIONS OF IT GOVERNANCE AND REGULATORY COMPLIANCE

IT governance provides the institutional architecture through which organisations assign decision rights, establish accountability, control technology-related risk and ensure that information systems support strategic and regulatory objectives. Its foundation extends beyond IT management because governance determines who makes technology decisions, how those decisions are monitored, and how business, risk and stakeholder interests are reconciled. Brown and Grant's synthesis shows that IT governance developed from earlier research on IT decision rights and loci of control, eventually integrating structural and behavioural perspectives into a broader governance domain (Brown & Grant, 2005). For insurers, this distinction matters because technology decisions affect underwriting integrity, claims processing, customer data and regulatory assurance.

A regulatory-compliance perspective adds a second foundational layer by connecting governance structures with legally and professionally defined obligations. In technology-dependent firms, compliance requires controls translating regulatory requirements into operational rules, responsibilities, evidence trails and monitoring. Hardy demonstrates that COBIT can connect IT value delivery with legal, regulatory and compliance requirements by providing control objectives that help management structure responsibilities and demonstrate accountability (Hardy, 2006). This logic is particularly relevant to insurers, where regulators expect reliable records, controlled access to sensitive information, continuity of critical systems and demonstrable oversight of technology-supported processes.

The Nigerian context requires these principles to be interpreted through the country's institutional and corporate-governance environment. Governance effectiveness depends not merely on adopting formal codes but on the interaction between regulatory structures, organisational behaviour, enforcement capacity and prevailing institutional practices. Okike's examination of corporate governance in Nigeria identifies weaknesses in institutional arrangements and governance mechanisms that can limit effective oversight despite regulatory prescriptions (Okike, 2007). Applied to Nigerian insurance firms, this suggests that IT governance frameworks must be embedded within board accountability, internal audit, risk management and management-control processes rather than treated as technical documentation maintained only by IT departments.

Information security constitutes another core foundation because regulatory compliance increasingly depends on the confidentiality, integrity and availability of information assets. Insurance organisations process extensive personal, financial and risk-related information, making security governance inseparable from enterprise governance. Von Solms argues that COBIT and information-security standards can perform complementary roles, with COBIT providing governance and control orientation while security standards offer more detailed protective practices (von Solms, 2005). This supports an integrated approach in Nigerian insurance firms whereby governance establishes authority, risk ownership and control expectations, while standards determine how safeguards are implemented and evaluated.

The practical relevance of formal governance frameworks is reinforced by evidence from developing economies. In Saudi organisations, COBIT processes were widely perceived as important, yet implementation frequently lagged behind perceived importance where organisational capability and governance maturity were insufficient (Abu-Musa, 2009). This gap is instructive for Nigerian insurers because compliance depends on more than framework recognition. Policies must be translated into functioning processes covering access management, change control, continuity, incident handling, performance monitoring and audit support. Governance maturity therefore reflects the extent to which prescribed controls are institutionalised, consistently executed and supported by management.
From an accounting and assurance perspective, IT governance also provides mechanisms for protecting information quality and supporting dependable reporting. Wilkin and Chenhall organise IT governance around strategic alignment, risk management, resource management, value delivery and performance measurement, demonstrating that

governance spans strategic and control-oriented dimensions (Wilkin & Chenhall, 2010). These dimensions intersect with insurance regulation because financial and prudential reporting increasingly relies on automated systems, integrated databases and technology-enabled controls. Weak governance can therefore compromise the accuracy, traceability and reliability of information upon which regulators, auditors and boards depend.

Institutional theory further explains why regulated organisations adopt governance structures even when their immediate economic benefits are difficult to quantify. Organisations operate under coercive pressures from regulators, normative pressures from professions and standards bodies, and mimetic pressures arising from accepted industry practice. Mignerat and Rivard show that institutional perspectives help explain information-system adoption where organisational choices are shaped by wider rules, norms and legitimacy expectations (Mignerat & Rivard, 2009). For Nigerian insurers, COBIT- and ITIL-aligned practices may therefore function simultaneously as mechanisms of operational discipline, regulatory conformity and organisational legitimacy within an increasingly formalised financial-services environment.

Effective compliance also requires governance mechanisms capable of integrating technical, human and process-related dimensions of security. Carcary, Renaud, McLaughlin and O'Brien propose a capability-oriented information-security governance framework that enables organisations to assess maturity and identify weaknesses across governance and management practices (Carcary et al., 2016). Such maturity thinking applies to Nigerian insurance firms because control effectiveness cannot be inferred solely from the existence of policies. A mature governance environment requires assigned ownership, competent personnel, tested controls, management oversight, measurable performance, and continuous remediation. Finally, regulatory compliance must be sustained throughout operational processes rather than assessed retrospectively. Compliance-monitoring research demonstrates the importance of examining process execution against formal requirements and identifying deviations through structured monitoring mechanisms (Ly et al., 2015). In Nigerian insurance operations, this principle can be applied to claims authorisation, policy administration, user-access management, system changes, data handling and regulatory reporting. The foundations of IT governance and compliance therefore rest on coordinated decision rights, controls, standards, monitoring, accountability and institutional legitimacy through which technology-enabled insurance activities remain aligned with regulatory expectations.

III. NIGERIA'S INSURANCE REGULATORY AND DIGITAL GOVERNANCE LANDSCAPE

Nigeria's insurance regulatory landscape has evolved through the interaction of statutory supervision, corporate-governance requirements, prudential expectations and market-development policies. Within this architecture, the National Insurance Commission (NAICOM) performs the central supervisory role, while insurers operate under requirements affecting licensing, capital adequacy, investments, claims obligations and market conduct. Evidence from the Nigerian industry indicates that regulatory instruments can materially shape sector performance, although their effects vary according to the particular instrument and prevailing economic conditions (Iheanacho, 2018). This makes regulatory compliance an operational capability rather than a periodic legal exercise because insurers must continuously translate supervisory expectations into controls governing financial, underwriting and technology-enabled activities.

The broader Nigerian governance environment also affects how effectively formal insurance requirements are implemented. Regulatory multiplicity has historically generated overlaps and inconsistencies among governance codes applicable to Nigerian companies, increasing uncertainty and potentially weakening compliance where institutional responsibilities are insufficiently harmonised (Osemeke & Adegbite, 2016). For insurance firms, such complexity is especially significant because governance obligations intersect with prudential supervision, financial reporting, internal control, customer protection and increasingly technology-dependent business processes. Digital governance therefore requires clear ownership of compliance

responsibilities across boards, executive management, risk functions, internal audit and information-technology units.

Institutional conditions further determine whether regulatory frameworks become embedded in organisational behaviour. Research on Sub-Saharan African corporate governance indicates that neither exclusively rules-based nor exclusively principles-based regulation is necessarily sufficient in weaker institutional environments; more effective arrangements may require contextualised co-regulation combining formal requirements, stakeholder participation and credible enforcement (Nakpodia et al., 2018). This insight is pertinent to Nigerian insurance because the effectiveness of digital controls depends not simply on written policies but also on managerial accountability, supervisory capability, professional competence and an organisational culture capable of sustaining control discipline.

The structure and maturity of African insurance markets additionally shape regulatory priorities. Comparative evidence across eight African countries, including Nigeria and South Africa, demonstrates heterogeneous relationships between insurance-market development and economic growth, reflecting variations in financial depth and institutional conditions (Alhassan & Biekpe, 2016). For Nigeria, the developing character of the insurance market creates a dual governance challenge: regulation must protect policyholders and preserve financial soundness while avoiding arrangements that unnecessarily impede innovation, distribution expansion and technology-enabled market deepening. Digital governance must consequently accommodate prudential discipline alongside responsible modernisation.

Digitalisation intensifies this balancing requirement. InsurTech innovations are reconfiguring insurance value creation through new forms of intermediation, data-driven services, digital interfaces and technologically enabled processes. A systematic examination of InsurTech innovations identifies numerous transformational capabilities affecting how insurers create and deliver value, demonstrating that digitalisation extends beyond routine automation to encompass business-model and industry-level transformation (Stoeckli, Dremel & Uebernickel, 2018). Nigerian insurers adopting comparable technologies therefore confront governance questions relating to system ownership, data quality, outsourcing, access rights, algorithmic processes, change management and the traceability of technology-supported decisions.

Digital finance also creates important regulatory trade-offs. Although digital channels can reduce transaction costs, widen access and improve service convenience, their expansion may generate concerns regarding cyber vulnerability, consumer protection, operational dependence and financial stability when governance safeguards do not develop correspondingly (Ozili, 2018). Within Nigerian insurance, these tensions become increasingly relevant as electronic payments, mobile platforms, online policy administration and digitally mediated customer interactions become integrated into core operations. Effective digital governance must therefore connect innovation decisions with information-security controls, operational resilience, accountability and dependable regulatory reporting.

Emerging technologies further increase the significance of verifiable digital records. Blockchain-based research into auto-insurance claims demonstrates how distributed architectures can strengthen record integrity, constrain unauthorised alteration and improve the verifiability of interactions among parties involved in claims adjudication (Oham et al., 2018). Although such technologies do not eliminate governance risk, they illustrate how technological design can embed auditability and evidence preservation within insurance processes. For Nigerian insurers, comparable principles are relevant to claims administration, fraud management and regulatory assurance, provided that technological adoption remains subject to clear control ownership, security safeguards and supervisory oversight.

International insurance experience additionally demonstrates why digital governance must remain connected to prudential risk oversight. Insurance institutions may transmit risk through interconnected financial activities, non-traditional products and relationships with other financial-sector entities,

creating supervisory considerations extending beyond individual-firm solvency (Cummins & Weiss, 2014). As Nigerian insurers deepen technological integration with banks, payment infrastructures, technology vendors and wider data ecosystems, governance must increasingly address both conventional insurance obligations and technology-mediated dependencies. IT governance therefore occupies an increasingly important position at the intersection of regulatory compliance, enterprise risk management and digital transformation within Nigeria's evolving insurance landscape.

IV. COBIT FOR GOVERNANCE, RISK, CONTROL, AND COMPLIANCE

COBIT provides an integrated architecture through which organisations can connect enterprise objectives with the governance and management of information technology. Its significance to regulated insurance firms lies in its capacity to convert broad strategic, fiduciary and regulatory expectations into structured governance processes, responsibilities, information requirements and performance measures. Rather than positioning technology as an isolated operational function, COBIT 5 conceptualises enterprise governance of IT as an end-to-end responsibility incorporating stakeholder needs, value creation, risk optimisation and resource stewardship. Its separation of governance from management further clarifies the respective roles of boards and executives in evaluating priorities, directing organisational action and monitoring outcomes (De Haes, Van Grembergen & Debreceny, 2013).

For Nigerian insurance firms, such clarity is particularly important because technology increasingly underpins premium administration, underwriting, claims settlement, accounting, customer information and regulatory reporting. Governance weaknesses can therefore migrate rapidly from the IT environment into financial, operational and compliance domains. Although not COBIT-specific, Nigerian corporate-governance evidence demonstrates that governance structures and board arrangements materially influence organisational outcomes, reinforcing the importance of clearly allocated oversight responsibilities and effective monitoring mechanisms (Ehikioya, 2009). COBIT can extend this governance logic into information technology by defining ownership for technology-related decisions, risks, controls and performance.

Risk optimisation represents a central element of the framework. COBIT enables enterprises to connect business risks with technology dependencies and to identify processes requiring preventive, detective and corrective controls. Empirical investigation of COBIT-based IT project management demonstrates that structured control frameworks can strengthen the specification and application of control mechanisms across complex technology initiatives (Bernroider & Ivanov, 2011). In insurance organisations, this principle applies beyond projects to system acquisition, software changes, third-party services, access management, cybersecurity, data processing and business continuity, where unmanaged technology risks may produce regulatory and financial consequences.

COBIT is equally significant as an internal-control architecture. Its control logic allows auditors and management to assess whether IT processes provide reasonable assurance that organisational objectives will be achieved and undesirable events identified or addressed. Experimental evidence supports the conceptual validity of COBIT as an internal-control framework and demonstrates its usefulness for structuring assessments of IT-related controls in audit settings (Tuttle & Vandervelde, 2007). Such systematic control assessment is valuable to insurers because regulatory compliance increasingly requires evidence that systems are not merely operational but appropriately authorised, protected, monitored and capable of producing reliable records.

Financial reporting provides a particularly important application. International evidence indicates that several COBIT processes are considered highly important for effective internal control over financial reporting, especially those associated with security, change management, data management, risk assessment and control monitoring (Kerr & Murthy, 2013). For Nigerian insurers, these functions intersect directly with the integrity of financial statements, solvency information, premium records and regulatory submissions. COBIT therefore provides a bridge between technology controls and the wider assurance

environment on which boards, auditors and regulators depend.

The framework can also strengthen compliance by complementing traditional corporate internal-control arrangements. Analysis of COBIT within financial-reporting control systems demonstrates that its IT-focused control objectives can address technology-related control weaknesses that broader internal-control frameworks may not capture with comparable specificity (Rubino & Vitolla, 2014). This is particularly pertinent where insurance processes are extensively automated, and compliance evidence is generated through interconnected applications and databases.

African experience further demonstrates COBIT's potential to translate general governance principles into actionable technology practices. In South Africa, COBIT 5 has been shown to provide detailed governance activities capable of supporting implementation of the IT-governance principles contained in King III, thereby connecting board-level expectations with practical governance mechanisms (Maseko & Marx, 2016). Similar contextual adaptation is important for Nigerian insurers rather than adopting COBIT mechanically without regard to local regulatory priorities, organisational capability and governance maturity.

Governance maturity ultimately determines whether formal controls produce substantive assurance. Research indicates that higher IT-governance maturity is associated with greater transparency in governance disclosure, suggesting that institutionalised governance processes strengthen an organisation's ability to demonstrate its technology oversight arrangements (Joshi et al., 2018). Moreover, COBIT-based evidence identifies alignment and information security among the major management concerns addressed through coordinated governance and management processes (Huygh et al., 2018). Within Nigerian insurance, COBIT can consequently provide a coherent mechanism for linking board oversight, technology risk, internal control, security, accountability and regulatory assurance within a single governance structure.

V. ITIL FOR RELIABLE AND COMPLIANT IT SERVICES

ITIL provides a structured approach to information technology service management by organising service delivery around repeatable processes, defined responsibilities, measurable performance and continual improvement. Its relevance to Nigerian insurance firms arises from the dependence of underwriting, premium administration, claims processing, customer portals and regulatory reporting on stable and recoverable digital services. Importantly, ITIL is not itself a regulatory compliance framework; rather, it creates operational disciplines through which organisations can demonstrate that technology services are controlled, monitored and continually improved. A systematic review of ITSM implementation research identifies process formalisation, organisational involvement and implementation capability as central considerations in translating service-management frameworks into sustainable practice (Iden & Eikebrokk, 2013).

Reliability is strengthened when ITIL practices replace fragmented technical responses with coordinated service-management routines. Incident management restores normal service after disruption, problem management seeks underlying causes, while change and configuration controls reduce the likelihood that poorly governed modifications compromise production environments. Empirical work on proactive IT operations demonstrates that mature service providers benefit from clearly documented incident and problem processes, defined responsibilities, service-level mechanisms and systematic use of feedback and performance information (Jäntti & Cater-Steel, 2017). For insurers, these practices can reduce interruptions to claims systems, policy databases and customer-facing channels while creating traceable records of operational events.

ITIL also contributes to compliance through disciplined change, access, continuity and service-level management. Regulatory assurance depends partly on the ability to show that material system changes are authorised, incidents are escalated, services are restored within acceptable periods and recurring weaknesses are subjected to corrective

action. Evidence from successful ITIL implementations in the United States and Australia indicates that senior-management commitment, training, communication, process ownership and appropriate implementation strategies are critical to institutionalising service-management practices (Pollard & Cater-Steel, 2009). These conditions are especially important where Nigerian insurers must coordinate IT personnel, compliance officers, internal auditors, business units and external service providers. Service-management maturity is equally important because partial adoption can produce documentation without dependable operational behaviour. International evidence indicates that greater ITIL implementation maturity is associated with increased realisation of benefits and a reduction in perceived implementation challenges, suggesting that value develops progressively as processes become embedded across the organisation (Marrone & Kolbe, 2011). For Nigerian insurance firms, maturity therefore requires more than adopting terminology; service controls must be integrated with governance, risk management, audit and regulatory reporting.

Performance measurement converts ITIL practices into evidence of service reliability. Metrics covering service availability, incident resolution, recurring problems, change success, service-level achievement and customer satisfaction allow management to identify deterioration before it generates material operational exposure. Cross-country research demonstrates that ITSM benefits and performance measurement are closely connected, although organisations vary considerably in the measures used and their ability to link technical indicators with business outcomes (Gacenga, Cater-Steel & Toleman, 2010). Insurance firms can use such measures to establish accountable thresholds for critical services and support defensible oversight of outsourced technology.

The Nigerian insurance context reinforces the importance of timeliness and dependable service execution. Although not an ITIL study, research on claims handling in Nigeria shows that effectiveness, efficiency and promptness are fundamental to claims-management performance and organisational productivity (Yusuf & Ajemunigbohun, 2015). ITIL-aligned incident, request, availability and service-level practices can support these operational attributes where claims processes depend on digital platforms. Similarly, South African evidence, while not ITIL-specific, indicates that system quality and user satisfaction influence the perceived benefits of organisational information systems (Serumaga-Zake, 2017). This wider African perspective underscores why compliant service management must remain user-oriented as well as control-oriented. Within Nigerian insurance, ITIL can therefore operationalise governance expectations through reliable service delivery, auditable process execution, controlled change, resilient support arrangements and measurable service performance under evolving Nigerian regulatory compliance expectations.

VI. INTEGRATING COBIT AND ITIL FOR ENTERPRISE COMPLIANCE

The integration of COBIT and ITIL offers a coherent means of connecting enterprise-level governance with the operational disciplines required for reliable technology services. In regulated insurance firms, this relationship is particularly important because compliance obligations depend simultaneously on strategic accountability, risk oversight, auditable controls and consistent execution of IT processes. COBIT establishes governance objectives, control expectations and performance responsibilities, whereas ITIL provides detailed practices for service design, transition, operation and continual improvement. Research comparing established frameworks indicates that no single framework comprehensively addresses governance, service management and information security; coordinated implementation can therefore reduce functional gaps and improve control coverage (Sahibudin, Sharifi & Ayat, 2008).

A central advantage of integration is the creation of traceability from board-level objectives to operational activities. Governance requirements concerning availability, confidentiality, change control, incident handling and continuity can be translated into ITIL-aligned service practices, while COBIT supplies the mechanisms for evaluating whether those practices satisfy enterprise objectives. Integrated governance research similarly argues that effective IT governance requires a clear interface between governance and

management rather than treating them as disconnected domains (Pereira & Mira da Silva, 2012). For Nigerian insurers, such an interface can establish clearer accountability between boards, executive management, risk functions, compliance teams, internal audit and technology units.

Integration also supports maturity assessment and targeted improvement. A practical COBIT–ITIL assessment can identify weaknesses in specific governance and service-management processes, establish desired capability levels and prioritise remediation according to business importance. Evidence from a public-sector communication environment demonstrates how COBIT and ITIL can be combined to assess capability and formulate improvement priorities where governance and service performance are interdependent (Ekanata & Girsang, 2017). In insurance, comparable mapping can connect regulatory requirements with service controls, responsible owners, evidence sources, performance indicators and remediation actions.

Compliance effectiveness also depends on unifying governance, risk and control information. Enterprise GRC research demonstrates the value of systematically evaluating relationships among governance, risk management and compliance controls rather than managing them as isolated functions (Ramalingam, Arun & Anbazhagan, 2018). Applied to Nigerian insurance, an integrated COBIT–ITIL architecture can support a common control environment in which technology risks identified through governance processes are linked to operational procedures for incidents, changes, access, availability and continuity. This improves audit readiness because regulatory obligations can be traced to documented processes and measurable evidence.

Nevertheless, framework integration must remain context-sensitive. South African evidence shows that organisations may face uncertainty when selecting and implementing competing IT governance frameworks, with adoption influenced by organisational circumstances and stakeholder perceptions (Batyashe & Iyamu, 2017). Nigerian insurance firms should therefore avoid mechanically implementing every COBIT and ITIL practice. Controls should instead be tailored according to regulatory exposure, organisational scale, technology dependence, outsourcing arrangements and governance maturity.

A Nigerian-linked perspective further emphasises that governance effectiveness develops through organisational learning, shared knowledge and the capacity to assimilate governance practices into decision-making routines (Ajayi & Hussin, 2018). Accordingly, COBIT–ITIL integration should be treated as an institutional capability rather than a documentation exercise. When governance objectives, service processes, risk registers, compliance obligations, audit evidence and performance measures are deliberately connected, Nigerian insurers can create a governance-to-operations chain that improves control consistency, regulatory transparency and resilience while preserving sufficient flexibility for evolving supervisory and technological requirements. This alignment also reduces duplicated controls, clarifies escalation pathways and enables compliance monitoring to draw on the same operational evidence used for day-to-day service assurance.

VII. COBIT AND ITIL IMPACT ON REGULATORY COMPLIANCE

The regulatory value of COBIT and ITIL lies in their capacity to convert broad governance expectations into repeatable, auditable and accountable technology practices. COBIT strengthens enterprise oversight by clarifying decision rights, control ownership and monitoring responsibilities, whereas ITIL concentrates on the disciplined management of technology-enabled services. Effective IT governance is associated with senior-management involvement, a culture of compliance and strong communication mechanisms, indicating that formal frameworks generate value when embedded within organisational behaviour rather than treated as documentation exercises (Ali & Green, 2012). For insurers, this translation is particularly important because regulatory obligations increasingly depend on digital evidence, reliable information flows, controlled system access, resilient service delivery and the demonstrable effectiveness of technology-enabled internal controls.

For insurance firms, COBIT can improve compliance assurance by establishing structured controls for planning, acquisition, service delivery, risk monitoring and performance evaluation. Its process architecture enables management and auditors to

identify control gaps, define capability targets and trace technology activities to business requirements. Evidence from a financing company shows that COBIT 5 can be applied to evaluate project-governance capability and identify areas requiring improvement, demonstrating its practical usefulness in financially regulated environments where control evidence and accountability are essential (Rooswati & Legowo, 2018).

ITIL contributes to regulatory compliance through operational consistency. Incident, change, problem, availability and continuity practices help organisations demonstrate that disruptions are recorded, system modifications are authorised, and service weaknesses are systematically corrected. A study of financial-sector organisations in Peru found that greater use of organisational change-management practices was associated with higher levels of ITIL compliance, illustrating that effective implementation depends on institutionalising processes, responsibilities and behavioural change rather than merely adopting framework terminology (Yamakawa et al., 2012).

The impact of ITIL is strengthened when service management is connected explicitly to governance. Service governance establishes accountability, decision authority and performance oversight, while service management operationalises these expectations through day-to-day processes. Research involving Finnish service providers indicates that neglecting governance while focusing only on service management can create difficulties in performance measurement, role definition, resource allocation and process improvement, thereby weakening the assurance value of otherwise well-designed service practices (Jäntti & Hotti, 2016).

This governance-to-service relationship is especially relevant to Nigerian insurance firms because technology increasingly supports claims processing, accounting, customer administration and information exchange. Although not a COBIT- or ITIL-specific study, Nigerian evidence shows that technological service delivery significantly improves operational efficiency, information timeliness and service effectiveness in insurance companies (Owolabi, 2018). These findings provide contextual justification for formal governance and service-management frameworks: as dependence on digital systems increases, unmanaged technology processes can become compliance vulnerabilities, while disciplined controls can improve traceability, reliability and regulatory responsiveness.

Comparable African insurance evidence also demonstrates that operational controls have direct implications for organisational performance. In East African property and casualty insurance companies, underwriting and claims-management practices were found to influence performance, highlighting the importance of controlled, timely and accountable operational processes (Angima & Mwangi, 2017). Within Nigerian insurance, COBIT and ITIL can therefore influence regulatory compliance through complementary pathways: COBIT provides governance, risk and control assurance, while ITIL embeds dependable service practices. Their impact is most pronounced where framework requirements are integrated with internal audit, enterprise risk management, compliance monitoring, management reporting and continuous improvement, creating defensible evidence that technology-dependent insurance processes remain controlled and aligned with organisational and regulatory expectations.

VIII. IMPLEMENTATION CHALLENGES, EMERGING TRENDS, AND RESEARCH PRIORITIES

Implementing COBIT and ITIL within Nigerian insurance firms presents challenges extending beyond the technical selection of governance and service-management processes. Successful adoption requires executive commitment, competent personnel, clearly allocated responsibilities, organisational learning, financial resources and an institutional culture capable of sustaining controls after initial implementation. Evidence from Tanzania demonstrates that senior-management support, stakeholder involvement, effective communication and appropriate management of IT infrastructure significantly influence IT-governance performance in resource-constrained environments (Nfuka & Rusu, 2011). These considerations are pertinent to Nigerian insurers, where governance maturity may vary considerably

between large, technologically sophisticated firms and smaller operators with limited specialist capability.

Framework complexity represents another implementation concern. COBIT contains extensive governance and management objectives, and indiscriminate adoption may generate excessive documentation, implementation costs and control burdens without corresponding regulatory value. Expert-based research on COBIT 5 therefore supports selective implementation through a minimum governance baseline tailored to organisational needs rather than uniform deployment of every available process (Bartens et al., 2015). Nigerian insurers should consequently prioritise controls according to regulatory exposure, information sensitivity, business criticality, outsourcing dependence and technology risk.

ITIL adoption presents related organisational difficulties because service-management improvement requires behavioural and procedural change alongside technical configuration. Critical success factors identified for ITIL implementation include management involvement, staff training, communication, process ownership, appropriate technology and systematic implementation planning (Ahmad & Shamsudin, 2013). These requirements become particularly significant where legacy applications, fragmented service responsibilities and insufficient documentation constrain process standardisation. Insurers must therefore avoid treating ITIL implementation as a certification exercise and instead embed service practices within daily operational accountability.

The available ITIL evidence also exposes an important research limitation. Mapping of international scholarship demonstrates substantial concentration on implementation practices and organisational benefits, while revealing continuing opportunities for more rigorous examination of framework application across different industries and institutional environments (De Barros et al., 2015). Nigeria's insurance industry remains particularly suitable for contextual research examining whether international service-management assumptions remain valid under local infrastructural, regulatory, skills and organisational conditions.

Infrastructure reliability adds a distinctive Nigerian implementation dimension. Although the study is not concerned with IT governance or insurance and should not be interpreted as direct COBIT/ITIL evidence, Sunday & Omoegun (2018) identify persistent electricity-supply constraints and the operational importance of alternative energy solutions within Nigerian enterprises. For digitally dependent insurers, unreliable supporting infrastructure can undermine system availability, disaster recovery, service-level performance and business continuity irrespective of the sophistication of formal governance controls. Future governance models should therefore integrate technology governance with physical infrastructure resilience rather than assuming uninterrupted operating conditions.

Emerging digital finance technologies will further alter the compliance environment. FinTech research identifies rapid development in digitally enabled financial products, platforms, technologies and institutional arrangements, while emphasising significant gaps requiring interdisciplinary investigation (Gomber, Koch & Siering, 2017). For Nigerian insurers, cloud services, automated underwriting, advanced analytics, application programming interfaces, mobile platforms and emerging distributed technologies create opportunities for efficiency but also introduce questions concerning data ownership, third-party accountability, cybersecurity, algorithmic oversight and regulatory traceability. COBIT and ITIL implementations will consequently need to evolve from predominantly internally controlled environments toward governance structures capable of overseeing increasingly interconnected digital ecosystems.

Research priorities should also move beyond determining whether frameworks have merely been adopted. Empirical evidence from Brazilian firms indicates that strategic alignment, value delivery, risk management and performance management contribute positively to IT-governance effectiveness, demonstrating the importance of examining governance outcomes rather than implementation status alone (Lunardi et al., 2017). Future Nigerian studies should therefore measure COBIT and ITIL maturity against regulatory findings, audit outcomes, incident frequency, system availability, control

deficiencies, claims-processing reliability and compliance costs. Longitudinal and comparative studies across insurers of different sizes would be particularly valuable. Such research could establish whether integrated COBIT–ITIL practices produce measurable compliance advantages, determine which controls provide greatest regulatory value, and support development of a context-sensitive governance maturity model suited to Nigeria's evolving insurance and digital-risk environment.

IX. CONCLUSION

This review has demonstrated that effective information technology governance is fundamental to regulatory compliance, operational resilience, and accountable digital transformation within Nigerian insurance firms. The study's aim was achieved by critically examining how COBIT and ITIL provide complementary structures for governing technology, managing service delivery, controlling risk, and supporting compliance obligations. The analysis established that COBIT contributes strategic oversight, control design, risk optimisation, performance monitoring, and auditability, while ITIL strengthens incident management, change control, service continuity, availability, and continual improvement. Their integration therefore creates a governance-to-operations architecture capable of aligning board-level expectations with daily technology practices.

The review further showed that Nigeria's insurance environment presents distinctive implementation pressures, including regulatory complexity, uneven governance maturity, legacy systems, infrastructure constraints, skills shortages, cybersecurity exposure, and growing dependence on digital platforms. These conditions reinforce the need for context-sensitive rather than mechanical adoption of international frameworks. Evidence examined across the study also indicates that governance effectiveness depends on executive sponsorship, clearly assigned responsibilities, competent personnel, measurable controls, and sustained organisational commitment.

The principal recommendation is that Nigerian insurers should adopt a phased, risk-based COBIT–ITIL integration model linked explicitly to regulatory obligations, internal audit, enterprise risk management, and business continuity. Firms should establish governance maturity assessments, define control ownership, strengthen service-level monitoring, and maintain evidence trails for technology-related compliance activities. Regulators should encourage proportionate governance expectations that recognise differences in organisational scale and digital complexity while promoting minimum control baselines across the sector. Investment in cybersecurity capability, workforce development, resilient infrastructure, and third-party oversight should also be prioritised. Future research should empirically test the relationship between framework maturity, regulatory findings, service reliability, compliance costs, and operational performance, thereby supporting a more evidence-based governance model for Nigeria's evolving insurance industry. Such evidence would help policymakers refine governance interventions while preserving innovation, accountability, consumer protection, and institutional resilience.

REFERENCES

[1] Abu-Musa, A.A. (2009) 'Exploring the importance and implementation of COBIT processes in Saudi organizations: An empirical study', Information Management & Computer Security, 17(2), pp. 73–95. https://doi.org/10.1108/09685220910963974. (Emerald Publishing)

[2] Adegbite, E. (2012) 'Corporate governance regulation in Nigeria', Corporate Governance: The International Journal of Business in Society, 12(2), pp. 257–276. https://doi.org/10.1108/14720701211214124. (Northumbria University Research Portal)

[3] Adesemowo, A.K., Von Solms, R. and Botha, R.A. (2016) 'Safeguarding information as an asset: Do we need a redefinition in the knowledge economy and beyond?', South African Journal of Information Management, 18(1), a706. https://doi.org/10.4102/sajim.v18i1.706.

[4] Aduloju, S.A. (2014) 'Information technology managerial capabilities and customer service

performance among insurance firms in Nigeria', SAGE Open, 4(4), article 2158244014561198. https://doi.org/10.1177/2158244014561198. (Sage Journals)

[5] Ahmad, N. and Shamsudin, Z.M. (2013) 'Systematic approach to successful implementation of ITIL', Procedia Computer Science, 17, pp. 237–244. https://doi.org/10.1016/j.procs.2013.05.032.

[6] Ajayi, B.A. and Hussin, H. (2018) 'Conceptualizing information technology governance model for higher education: An absorptive capacity approach', Bulletin of Electrical Engineering and Informatics, 7(1), pp. 117–124. https://doi.org/10.11591/eei.v7i1.898.

[7] Alhassan, A.L. and Biekpe, N. (2016) 'Insurance market development and economic growth: Exploring causality in 8 selected African countries', International Journal of Social Economics, 43(3), pp. 321–339. https://doi.org/10.1108/IJSE-09-2014-0182. (Emerald Publishing)

[8] Ali, S. and Green, P. (2012) 'Effective information technology (IT) governance mechanisms: An IT outsourcing perspective', Information Systems Frontiers, 14(2), pp. 179–193. https://doi.org/10.1007/s10796-009-9183-y.

[9] Alreemy, Z., Chang, V., Walters, R. and Wills, G. (2016) 'Critical success factors (CSFs) for information technology governance (ITG)', International Journal of Information Management, 36(6), pp. 907–916. https://doi.org/10.1016/j.ijinfomgt.2016.05.017.

[10] Angima, C.B. and Mwangi, M. (2017) 'Effects of underwriting and claims management on performance of property and casualty insurance companies in East Africa', European Scientific Journal, 13(13), pp. 358–373. https://doi.org/10.19044/esj.2017.v13n13p358.

[11] Bartens, Y., De Haes, S., Lamoen, Y., Schulte, F. and Voss, S. (2015) 'On the way to a minimum baseline in IT governance: Using expert views for selective implementation of COBIT 5', 2015 48th Hawaii International Conference on System Sciences, pp. 4554–4563. https://doi.org/10.1109/HICSS.2015.543.

[12] Batyashe, T.N. and Iyamu, T. (2017) 'Examining IT governance through diffusion of innovations: A case of a South African telecom', Information Resources Management Journal, 30(3), pp. 26–40. https://doi.org/10.4018/IRMJ.2017070102.

[13] Bernroider, E.W.N. and Ivanov, M. (2011) 'IT project management control and the Control Objectives for IT and related Technology (CobiT) framework', International Journal of Project Management, 29(3), pp. 325–336. https://doi.org/10.1016/j.ijproman.2010.03.002.

[14] Biener, C., Eling, M. and Wirfs, J.H. (2015) 'Insurability of cyber risk: An empirical analysis', The Geneva Papers on Risk and Insurance – Issues and Practice, 40(1), pp. 131–158. https://doi.org/10.1057/gpp.2014.19. (Springer)

[15] Brown, A.E. and Grant, G.G. (2005) 'Framing the frameworks: A review of IT governance research', Communications of the Association for Information Systems, 15, pp. 696–712. https://doi.org/10.17705/1CAIS.01538. (AIS eLibrary)

[16] Carcary, M., Renaud, K., McLaughlin, S. and O'Brien, C. (2016) 'A framework for information security governance and management', IT Professional, 18(2), pp. 22–30. https://doi.org/10.1109/MITP.2016.27. (Mary Immaculate College)

[17] Cummins, J.D. and Weiss, M.A. (2014) 'Systemic risk and the U.S. insurance sector', Journal of Risk and Insurance, 81(3), pp. 489–528. https://doi.org/10.1111/jori.12039. (Wiley Online Library)

[18] De Barros, M.D., Salles, C.A.L., Gomes, C.F.S., Da Silva, R.A. and Costa, H.G. (2015) 'Mapping of the scientific production on the ITIL application published in the national and international literature', Procedia Computer Science, 55, pp. 102–111. https://doi.org/10.1016/j.procs.2015.07.013.

[19] De Haes, S. and Van Grembergen, W. (2009) 'An exploratory study into IT governance implementations and its impact on business/IT alignment', Information Systems Management, 26(2), pp. 123–137.

https://doi.org/10.1080/10580530902794786. (Taylor & Francis Online)

[20] De Haes, S., Huygh, T., Joshi, A.S. and Van Grembergen, W. (2016) 'Adoption and impact of IT governance and management practices: A COBIT 5 perspective', International Journal of IT/Business Alignment and Governance, 7(1), pp. 50–72. https://doi.org/10.4018/IJITBAG.2016010104. (Open Universiteit research portal)

[21] De Haes, S., Van Grembergen, W. and Debreceny, R.S. (2013) 'COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities', Journal of Information Systems, 27(1), pp. 307–324. https://doi.org/10.2308/isys-50422.

[22] Ehikioya, B.I. (2009) 'Corporate governance structure and firm performance in developing economies: Evidence from Nigeria', Corporate Governance: The International Journal of Business in Society, 9(3), pp. 231–243. https://doi.org/10.1108/14720700910964307.

[23] Ejofodomi, O.A., Gideon, E.N., Oladipo, G.O. and Oshomah, E.R. (2014) 'Automated detection of architectural detection in mammograms using template matching', International Journal of Biomedical Science and Engineering, 2(1), pp. 1–6. https://doi.org/10.11648/j.ijbse.20140201.11. (sciencepg.com)

[24] Ekanata, A. and Girsang, A.S. (2017) 'Assessment of capability level and IT governance improvement based on COBIT and ITIL framework at communication center ministry of foreign affairs', 2017 International Conference on ICT for Smart Society (ICISS), pp. 1–7. https://doi.org/10.1109/ICTSS.2017.8288871.

[25] Eling, M. and Lehmann, M. (2018) 'The impact of digitalization on the insurance value chain and the insurability of risks', The Geneva Papers on Risk and Insurance – Issues and Practice, 43(3), pp. 359–396. https://doi.org/10.1057/s41288-017-0073-0. (IDEAS/RePEc)

[26] Eling, M. and Schnell, W. (2016) 'What do we know about cyber risk and cyber risk insurance?', The Journal of Risk Finance, 17(5), pp. 474–491. https://doi.org/10.1108/JRF-09-2016-0122. (Emerald Publishing)

[27] Gacenga, F., Cater-Steel, A. and Toleman, M. (2010) 'An international analysis of IT service management benefits and performance measurement', Journal of Global Information Technology Management, 13(4), pp. 28–63. https://doi.org/10.1080/1097198X.2010.10856525.

[28] Gomber, P., Koch, J.A. and Siering, M. (2017) 'Digital Finance and FinTech: Current research and future research directions', Journal of Business Economics, 87(5), pp. 537–580. https://doi.org/10.1007/s11573-017-0852-x.

[29] Hardy, G. (2006) 'Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges', Information Security Technical Report, 11(1), pp. 55–61. https://doi.org/10.1016/j.istr.2005.12.004. (ResearchGate)Huygh, T., De Haes, S., Joshi, A. and Van Grembergen, W. (2018) 'Answering key global IT management concerns through IT governance and management processes: A COBIT 5 view', Proceedings of the 51st Hawaii International Conference on System Sciences, pp. 5335–5344. https://doi.org/10.24251/HICSS.2018.665.

[30] Iden, J. and Eikebrokk, T.R. (2013) 'Implementing IT Service Management: A systematic literature review', International Journal of Information Management, 33(3), pp. 512–523. https://doi.org/10.1016/j.ijinfomgt.2013.01.004.

[31] Idris, A.A., Olumoko, T.A. and Ajemunigbohun, S.S. (2013) 'The role of information technology in customers' service delivery and firm performance: Evidence from Nigeria's insurance industry', International Journal of Marketing Studies, 5(4), p. 59. https://doi.org/10.5539/ijms.v5n4p59.

[32] Iheanacho, E. (2018) 'Insurance industry performance and the selected regulatory instruments in Nigeria', IOSR Journal of Economics and Finance, 9(6), pp. 67–77. https://doi.org/10.9790/5933-0906016777. (Europub)

[33] Jäntti, M. and Cater-Steel, A. (2017) 'Proactive management of IT operations to improve IT services', Journal of Information Systems and Technology Management, 14(2), pp. 191–218. https://doi.org/10.4301/S1807-17752017000200004.

[34] Jäntti, M. and Hotti, V. (2016) 'Defining the relationships between IT service management and IT service governance', Information Technology and Management, 17(2), pp. 141–150. https://doi.org/10.1007/s10799-015-0239-z.

[35] Jewer, J. and McKay, K.N. (2012) 'Antecedents and consequences of board IT governance: Institutional and strategic choice perspectives', Journal of the Association for Information Systems, 13(7), pp. 581–617. https://doi.org/10.17705/1jais.00301. (AIS eLibrary)

[36] Joshi, A., Bollen, L., Hassink, H., De Haes, S. and Van Grembergen, W. (2018) 'Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role', Information & Management, 55(3), pp. 368–380. https://doi.org/10.1016/j.im.2017.09.003.

[37] Kerr, D.S. and Murthy, U.S. (2013) 'The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: An international survey', Information & Management, 50(7), pp. 590–597. https://doi.org/10.1016/j.im.2013.07.012.

[38] Lunardi, G.L., Becker, J.L., Maçada, A.C.G. and Dolci, P.C. (2014) 'The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms', International Journal of Accounting Information Systems, 15(1), pp. 66–81. https://doi.org/10.1016/j.accinf.2013.02.001. (IDEAS/RePEc)

[39] Lunardi, G.L., Maçada, A.C.G., Becker, J.L. and Van Grembergen, W. (2017) 'Antecedents of IT governance effectiveness: An empirical examination in Brazilian firms', Journal of Information Systems, 31(1), pp. 41–57. https://doi.org/10.2308/isys-51626.

[40] Ly, L.T., Maggi, F.M., Montali, M., Rinderle-Ma, S. and van der Aalst, W.M.P. (2015) 'Compliance monitoring in business processes: Functionalities, application, and tool-support', Information Systems, 54, pp. 209–234. https://doi.org/10.1016/j.is.2015.02.007. (Eindhoven University Research Portal)

[41] Marnewick, C. and Labuschagne, L. (2011) 'An investigation into the governance of information technology projects in South Africa', International Journal of Project Management, 29(6), pp. 661–670. https://doi.org/10.1016/j.ijproman.2010.07.004. (University of Johannesburg)

[42] Marrone, M. and Kolbe, L.M. (2011) 'Impact of IT service management frameworks on the IT organization: An empirical study on benefits, challenges, and processes', Business & Information Systems Engineering, 3(1), pp. 5–18. https://doi.org/10.1007/s12599-010-0141-5.

[43] Marrone, M., Gacenga, F., Cater-Steel, A. and Kolbe, L. (2014) 'IT service management: A cross-national study of ITIL adoption', Communications of the Association for Information Systems, 34(1), pp. 865–892. https://doi.org/10.17705/1CAIS.03449.

[44] Maseko, L. and Marx, B. (2016) 'An analysis of COBIT 5 as a framework for the implementation of IT governance with reference to King III', Risk Governance & Control: Financial Markets & Institutions, 6(1), pp. 20–34. https://doi.org/10.22495/rgcv6i1art3.

[45] Mignerat, M. and Rivard, S. (2009) 'Positioning the institutional perspective in information systems research', Journal of Information Technology, 24(4), pp. 369–391. https://doi.org/10.1057/jit.2009.13. (Sage Journals)

[46] Nakpodia, F., Adegbite, E., Amaeshi, K. and Owolabi, A. (2018) 'Neither principles nor rules: Making corporate governance work in Sub-Saharan Africa', Journal of Business Ethics, 151(2), pp. 391–408. https://doi.org/10.1007/s10551-016-3208-5. (IDEAS/RePEc)

[47] Nfuka, E.N. and Rusu, L. (2011) 'The effect of critical success factors on IT governance performance', Industrial Management & Data

Systems, 111(9), pp. 1418–1448. https://doi.org/10.1108/02635571111182773.

[48] Oham, C., Jurdak, R., Kanhere, S.S., Dorri, A. and Jha, S. (2018) 'B-FICA: Blockchain-based framework for auto-insurance claim and adjudication', in 2018 IEEE International Congress on Cybermatics, pp. 1171–1180. https://doi.org/10.1109/Cybermatics_2018.2018.00210. (UNSW Sites)

[49] Okike, E.N.M. (2007) 'Corporate governance in Nigeria: The status quo', Corporate Governance: An International Review, 15(2), pp. 173–193. https://doi.org/10.1111/j.1467-8683.2007.00553.x. (Wiley Online Library)

[50] Osemeke, L. and Adegbite, E. (2016) 'Regulatory multiplicity and conflict: Towards a combined code on corporate governance in Nigeria', Journal of Business Ethics, 133(3), pp. 431–451. https://doi.org/10.1007/s10551-014-2405-3. (IDEAS/RePEc)

[51] Owolabi, A.O. (2018) 'Insurance products: Technological service delivery perspective', Business and Economic Research, 8(3), pp. 19–28. https://doi.org/10.5296/ber.v8i3.13238.

[52] Ozili, P.K. (2018) 'Impact of digital finance on financial inclusion and stability', Borsa Istanbul Review, 18(4), pp. 329–340. https://doi.org/10.1016/j.bir.2017.12.003. (OA Monitor Ireland)

[53] Pereira, R. and Mira da Silva, M. (2012) 'Designing a new integrated IT governance and IT management framework based on both scientific and practitioner viewpoint', International Journal of Enterprise Information Systems, 8(4), pp. 1–43. https://doi.org/10.4018/jeis.2012100101.

[54] Pollard, C. and Cater-Steel, A. (2009) 'Justifications, strategies, and critical success factors in successful ITIL implementations in U.S. and Australian companies: An exploratory study', Information Systems Management, 26(2), pp. 164–175. https://doi.org/10.1080/10580530902797540.

[55] Pooser, D.M., Browne, M.J. and Arkhangelska, O. (2018) 'Growth in the perception of cyber risk: Evidence from U.S. P&C insurers', The Geneva Papers on Risk and Insurance – Issues and Practice, 43(2), pp. 208–223. https://doi.org/10.1057/s41288-017-0077-9. (IDEAS/RePEc)

[56] Ramalingam, D., Arun, S. and Anbazhagan, N. (2018) 'A novel approach for optimizing governance, risk management and compliance for enterprise information security using DEMATEL and FoM', Procedia Computer Science, 134, pp. 365–370. https://doi.org/10.1016/j.procs.2018.07.197.

[57] Rooswati, R. and Legowo, N. (2018) 'Evaluation of IT project management governance using COBIT 5 framework in financing company', in 2018 International Conference on Information Management and Technology (ICIMTech), pp. 81–85. https://doi.org/10.1109/ICIMTech.2018.8528192.

[58] Rubino, M., Vitolla, F. and Garzoni, A. (2017) 'The impact of an IT governance framework on the internal control environment', Records Management Journal, 27(1), pp. 19–41. https://doi.org/10.1108/RMJ-03-2016-0007. (Emerald Publishing)

[59] Sahibudin, S., Sharifi, M. and Ayat, M. (2008) 'Combining ITIL, COBIT and ISO/IEC 27002 to design a comprehensive IT framework in organizations', 2008 Second Asia International Conference on Modelling & Simulation, pp. 749–753. https://doi.org/10.1109/AMS.2008.145.

[60] Serumaga-Zake, P.A.E. (2017) 'The role of user satisfaction in implementing a Business Intelligence System', South African Journal of Information Management, 19(1), a736. https://doi.org/10.4102/sajim.v19i1.736.

[61] Stoeckli, E., Dremel, C. and Uebernickel, F. (2018) 'Exploring characteristics and transformational capabilities of InsurTech innovations to understand insurance value creation in a digital world', Electronic Markets, 28(3), pp. 287–305. https://doi.org/10.1007/s12525-018-0304-7. (Springer)

[62] Sunday, E.A. and Omoegun, G.O. (2018) 'Integrating solar power solutions in small-scale manufacturing industries in Nigeria',

International Journal of Scientific Research in Science, Engineering and Technology, 4(8), pp. 832–853. https://doi.org/10.32628/IJSRSET23102175.

[63] Sutherland, E. (2017) 'Governance of cybersecurity – The case of South Africa', The African Journal of Information and Communication, 20, pp. 83–112. https://doi.org/10.23962/10539/23574. (Wits University)

[64] Talesh, S.A. (2018) 'Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses', Law & Social Inquiry, 43(2), pp. 417–440. https://doi.org/10.1111/lsi.12303. (Cambridge University Press)

[65] Veronica and Suryawan, A.D. (2017) 'Information technology service performance management using COBIT and an ITIL framework: A systematic literature review', 2017 International Conference on Information Management and Technology (ICIMTech), Yogyakarta, Indonesia, pp. 150–155. https://doi.org/10.1109/ICIMTech.2017.8273528.

[66] von Solms, B. (2005) 'Information security governance: COBIT or ISO 17799 or both?', Computers & Security, 24(2), pp. 99–104. https://doi.org/10.1016/j.cose.2005.02.002. (University of Johannesburg)

[67] Wilkin, C.L. and Chenhall, R.H. (2010) 'A review of IT governance: A taxonomy to inform accounting information systems', Journal of Information Systems, 24(2), pp. 107–146. https://doi.org/10.2308/jis.2010.24.2.107. (Monash University)

[68] Yamakawa, P., Obregón Noriega, C., Novoa Linares, A. and Vega Ramírez, W. (2012) 'Improving ITIL compliance using change management practices: A finance sector case study', Business Process Management Journal, 18(6), pp. 1020–1035. https://doi.org/10.1108/14637151211283393.

[69] Yusuf, T.O. and Ajemunigbohun, S.S. (2015) 'Effectiveness, efficiency, and promptness of claims handling process in the Nigerian insurance industry', European Journal of Business and Economics, 10(2), pp. 6–10. https://doi.org/10.12955/ejbe.v10i2.686.