# A Conceptual Framework for Developing Risk-Based Internal Control Models in the Insurance and Banking Sectors

OLAWOLE AKOMOLAFE[1], MICHAEL UZOMA AGU[2]
[1]*Nigeria Liability Insurance Pool, Lagos, Nigeria*
[2]*Shell Petroleum Development Company of Nigeria Limited*

***Abstract-*** ***Risk-based internal control (RBIC) is now a critical pillar of financial-sector governance, particularly within banking and insurance institutions whose risk exposures are complex, interdependent, and constantly evolving. Despite the existence of major regulatory doctrines such as Basel II/III and Solvency II, many institutions continue to rely on fragmented or compliance-oriented control systems that fail to align control processes with the organisation's risk profile. This paper develops a conceptual framework for RBIC tailored to the unique operational and regulatory environments of banking and insurance organisations. Drawing exclusively from literature published up to 2017, the study synthesises internal control theory, enterprise risk management (ERM), risk governance research, behavioural models, and financial regulation scholarship. The introduction and literature review critically examine the evolution of internal control, the emergence of risk-based approaches, sector-specific vulnerabilities, regulatory pressures, and implementation challenges. The conceptual framework integrates five core pillars: governance and architecture, risk identification and assessment, control design, information and communication infrastructure, and monitoring and assurance. The framework provides a structured and theoretically grounded approach to strengthening RBIC, enabling financial institutions to enhance resilience, accountability, and supervisory compliance.***

***Keywords:*** ***Risk-Based Internal Control, Risk Governance, Banking Internal Controls, Insurance Risk Management, Enterprise Risk Management, Internal Audit.***

## I. INTRODUCTION

Internal control remains one of the most important mechanisms supporting organisational governance, transparency, accountability, and operational integrity. In the financial sector—where risks are uniquely interconnected, fast-moving, and capable of generating systemic consequences, the role of internal control becomes even more significant [1]. Insurance and banking institutions operate under heavy regulation, manage extensive financial assets, and carry liabilities whose management depends on effective risk identification, mitigation, and monitoring [2], [3]. Within such environments, traditional compliance-centric internal control systems are no longer adequate. Instead, financial institutions require internal control frameworks that are explicitly risk-based, integrated, and aligned with organisational risk appetite and regulatory requirements [4], [5], [6].

The evolution from compliance-oriented to risk-based internal control (RBIC) reflects a broader shift in financial governance paradigms. Historically, internal controls in financial institutions emphasized adherence to procedures, segregation of duties, accuracy in transaction recording, and error prevention [7], [8]. Although these traditional controls remain essential, they are insufficient in isolation because they do not systematically capture emerging or rapidly changing risk exposures. The financial crisis of 2007–2008 exposed numerous shortcomings in conventional control systems, including failures in risk oversight, weak governance practices, poor risk culture, and insufficient board involvement in risk processes [9], [10]. These deficiencies resulted in large-scale collapses of banks and insurers across multiple jurisdictions. Studies documented failures in risk governance at institutions such as Lehman Brothers, AIG, Northern Rock, and several European banks,

where internal controls were either inadequate or unable to keep pace with evolving risk exposures [11], [12].

Following the crisis, regulatory bodies expanded supervisory expectations. The Basel Committee on Banking Supervision strengthened the internal control requirements embedded in Basel II and Basel III, emphasising the role of internal control in capital adequacy assessment, operational risk management, liquidity management, and market discipline [13], [14]. Similarly, the European Union implemented the Solvency II Directive, which introduced a risk-based framework for insurers, requiring formal risk management functions, internal controls, actuarial oversight, and the Own Risk and Solvency Assessment (ORSA) process [15], [16]. Both Basel III and Solvency II represent significant regulatory pressure for institutions to adopt structured, risk-sensitive internal control models.

In addition to regulatory drivers, the increasing complexity of financial products, the digitisation of financial services, and the rise of technology-facilitated risks have further underscored the need for more sophisticated RBIC systems. Banks now deploy online banking platforms, algorithmic trading systems, and automated credit scoring tools, while insurers increasingly rely on automated underwriting, telematics, and data-intensive actuarial models. These innovations bring enormous opportunities but also introduce new risks such as cyberattacks, system failures, algorithmic bias, data breaches, and operational disruptions. Internal control systems must therefore be capable of mitigating these emerging threats through the use of advanced monitoring systems, integrated information architectures, and dynamic risk assessment capabilities.

Despite the importance of RBIC, many institutions continue to struggle with implementation. Challenges vary widely and include fragmented organisational structures, poor information flows, lack of risk culture, insufficient board engagement, outdated technology, and inadequate risk assessment methodologies [17]. Empirical studies before 2018 repeatedly showed that many banks maintained “siloed” risk management approaches that prevented effective integration of internal control activities across departments [18], [19]. In the insurance sector, weaknesses were common in underwriting discipline, claims verification processes, actuarial modelling governance, and data management practices [20], [21], [22]. These challenges contribute to misaligned incentives, duplicated efforts, delayed reporting, and insufficient anticipation of emerging risks [23], [24].

Risk culture also plays a significant role. Research indicates that internal control failures often stem not from technical weaknesses but from poor organisational culture, lack of ethical leadership, inadequate communication channels, and reward systems that encourage excessive risk taking [25], [26], [27]. For example, banks involved in the mis-selling scandals of the 2010s consistently exhibited weak internal controls alongside dysfunctional performance incentive structures [28], [29]. These behavioural issues have been studied extensively in the auditing and risk literature, indicating the importance of integrating cultural and behavioural factors into RBIC models [30], [31].

Although substantial literature exists on internal control and risk management, there is a notable gap in integrated conceptual models specifically tailored to the banking and insurance sectors. Traditional frameworks such as the COSO Internal Control–Integrated Framework and the COSO ERM Framework provide strong foundations but are not sector-specific and do not fully address regulatory distinctions, operational complexities, and risk structures unique to banks and insurers. Similarly, while the ISO 31000 risk management standard offers guidance on risk assessment, it does not directly translate into internal control design. There is therefore a clear need for a conceptual RBIC framework that blends sector-specific regulatory requirements with governance theory, risk processes, information systems, and monitoring structures.

This paper addresses this gap by developing a conceptual framework for RBIC within the insurance and banking sectors. Drawing exclusively from pre-2018 literature, the study integrates knowledge from financial regulation, auditing, ERM, behavioral risk models, organizational governance, and information systems research. The conceptual framework advances understanding of RBIC by articulating how

governance architecture, risk assessment processes, control design principles, information and communication structures, and monitoring mechanisms interact to produce an integrated internal control environment.

This paper contributes to both theory and practice. From a theoretical perspective, it offers a comprehensive and structured conceptualization that synthesizes diverse strands of literature. From a practical perspective, it provides financial institutions with a blueprint for strengthening their internal control systems in alignment with risk exposure, regulatory expectations, and organizational strategy. Because the model emphasizes alignment, integration, and continuous monitoring, it is adaptable to institutions of varying size, complexity, and technological maturity.

The remainder of the paper is structured as follows. Section 2 presents a critical review of internal control and risk management literature up to 2017, highlighting the evolution of risk-based approaches, regulatory influences, sector-specific risks, and implementation challenges. Section 3 introduces the conceptual framework, detailing the five core pillars and their interactions. Section 4 discusses the framework's implications for practice and theory. Section 5 concludes by summarising the contribution of the work and suggesting areas for future research.

## II. LITERATURE REVIEW

The evolution of internal control theory and practice has been shaped by organizational governance expectations, regulatory developments, and the increasing complexity of financial-sector risks. Early conceptions of internal control, particularly those preceding the 1990s, tended to focus on recordkeeping accuracy, prevention of fraud, and procedural compliance. As organizations grew in scale and complexity, scholars and practitioners began to view internal control as a broader governance mechanism designed not only to support reliable financial reporting but also to enhance operational efficiency and enforce compliance with laws and regulations. This perspective was formalised in the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control–Integrated Framework of 1992, which became a dominant reference for both academic research and professional practice [1]. The framework introduced five interconnected components, control environment, risk assessment, control activities, information and communication, and monitoring, laying the conceptual foundation for modern internal control systems.

The COSO framework represented a shift from purely transaction-level controls toward a more holistic understanding of organisational governance. Subsequent revisions, including the 2013 update, further emphasised the alignment of internal control with organisational objectives, technological systems, and risk management practices [2]. However, while COSO provides a general structure for internal control, it does not explicitly account for the specialised risk environment of financial institutions. Banks and insurers operate under conditions of heightened uncertainty, are exposed to numerous internal and external risk drivers, and must adhere to sector-specific regulatory frameworks that introduce complex compliance obligations. As a result, scholars have argued that internal control systems in financial institutions must be tailored to address unique risks such as credit risk, underwriting risk, liquidity risk, market volatility, operational failures, and fraud [3], [4].

The emergence of enterprise risk management (ERM) in the early 2000s further influenced internal control thinking. COSO's 2004 ERM—Integrated Framework expanded internal control concepts by explicitly linking risk assessment processes with strategic planning, performance measurement, and governance structures [5]. ERM emphasised a top-down approach to risk identification, risk appetite definition, and continuous monitoring. This broadened perspective placed internal control within the larger context of enterprise governance, highlighting the necessity of aligning control activities with risk-taking objectives. ISO 31000, first released in 2009, contributed additional principles of structured risk identification, contextual analysis, risk evaluation, and risk treatment, reinforcing global convergence around integrated approaches to organisational risk management [6]. Together, these frameworks provided the intellectual foundations for the development of risk-based internal control (RBIC) systems.

The transition from traditional internal control to RBIC was accelerated by the financial scandals and corporate failures of the early 2000s, including Enron, WorldCom, HIH Insurance, and Parmalat. Investigations revealed widespread governance failures, weak oversight mechanisms, poor internal control governance, and a lack of risk-sensitive decision-making processes. These failures prompted regulators to strengthen internal control requirements, most notably through the Sarbanes–Oxley Act of 2002 in the United States, which imposed explicit obligations on management to certify the adequacy of internal control systems [7]. Section 404, in particular, underscored the importance of internal control over financial reporting and compelled organizations to integrate risk management considerations into their control assessments.

Within the financial sector, regulatory reforms following the global financial crisis of 2007–2008 had profound implications for internal control development. The Basel II framework, initially published in 2004, had already introduced risk-based capital requirements and emphasized the importance of internal risk assessments in credit risk and operational risk management [8]. Basel III, released in the wake of the crisis, strengthened these requirements by introducing liquidity standards, leverage ratios, enhanced disclosures, and more rigorous expectations regarding governance and internal control. Supervisory guidelines under Basel III highlighted the necessity for banks to maintain control systems that support accurate risk measurement, stress testing, limit management, and independent review [9]. The failure of several major banks during the crisis, including Lehman Brothers, Washington Mutual, and various European institutions, underscored the consequences of inadequate internal control and risk oversight [10], [11]. Studies identified weaknesses in credit underwriting controls, excessive reliance on flawed risk models, insufficient board oversight, and poor risk culture as key drivers of internal control failures [12], [13].

Similarly, in the insurance sector, the implementation of the Solvency II Directive in 2016 represented a major shift toward risk-based supervision. Solvency II introduced three pillars: quantitative requirements, qualitative requirements (including governance and internal control), and reporting and disclosure [14]. The second pillar explicitly requires insurers to maintain effective internal control systems, risk management functions, compliance functions, and actuarial functions. A core element of Solvency II is the Own Risk and Solvency Assessment (ORSA), which obliges insurers to conduct internal assessments of their risk profiles, solvency needs, and governance practices. ORSA operationalises risk-based control by requiring insurers to link risk assessment with internal control adequacy and capital management [15], [16].

In banking, internal control literature highlights credit risk controls, market risk controls, operational risk controls, and compliance oversight as critical domains requiring risk-based mechanisms. Credit risk controls involve borrower due diligence, credit scoring, collateral valuation, approval hierarchies, and ongoing monitoring [17]. Market risk controls center on ensuring limits on trading exposure, monitoring value-at-risk (VaR), stress testing, and verifying adherence to treasury policies [18], [19]. Operational risk controls address risks arising from system failures, fraud, process breakdowns, and external events. The Basel Committee has consistently emphasised the importance of operational controls such as segregation of duties, authorization procedures, real-time exception reporting, business continuity planning, and cybersecurity measures [20], [21]. Compliance and anti-money-laundering (AML) controls constitute another core domain, requiring mechanisms for customer identification, transaction monitoring, sanctions screening, and suspicious activity reporting [22], [23].

In the insurance sector, studies have identified underwriting controls, claims management controls, actuarial governance, investment oversight, and reinsurance controls as central elements of internal control systems. Underwriting controls ensure proper risk selection, adherence to pricing guidelines, and accuracy in policy documentation [24]. Claims controls require processes for validating claims, detecting fraud, assessing loss severity, and ensuring accurate settlement [25]. Actuarial controls involve model validation, assumption governance, data quality controls, and independent review of reserving methodologies [26]. Investment controls ensure compliance with investment mandates, diversification

requirements, asset–liability management (ALM) policies, and valuation standards [27]. Weaknesses in any of these control domains have historically contributed to insurer failures, including cases involving inadequate reserving, aggressive underwriting, and fraud [28], [29].

Risk governance plays a pivotal role in determining the effectiveness of internal control systems. The board of directors is responsible for defining risk appetite, approving internal control frameworks, and overseeing management's implementation of control activities. Research shows that institutions with strong board oversight, clear governance structures, and dedicated risk committees are more likely to maintain effective control systems and avoid catastrophic failures [32], [33]. Senior management is responsible for translating governance policies into operational control structures, ensuring adequate staffing, promoting risk culture, allocating resources, and integrating risk management into daily operations. Weak leadership commitment often results in fragmented controls, inconsistent implementation, and poor decision-making processes [30], [34].

The three lines of defence (3LoD) model has been widely adopted in financial institutions as a governance blueprint for internal control. Under this model, operational management constitutes the first line of defence, responsible for identifying and managing risks within business units. Risk management and compliance functions form the second line, overseeing the design of risk frameworks and monitoring adherence to policies. Internal audit serves as the third line, providing independent assurance regarding the effectiveness of both the first and second lines [35]. Although widely accepted, the 3LoD model has faced criticism for role ambiguity, siloed communication, inconsistent accountability, and weak coordination across departments [36], [37]. Studies suggest that without strong governance and integration, the 3LoD model may devolve into a formalistic rather than functional control structure [38], [39].

Behavioural and cultural factors also significantly influence internal control effectiveness. Scholars emphasize that risk culture defined as the shared norms, values, and behaviours that influence risk-related decision-making can either strengthen or undermine internal control systems [40], [41]. Poor risk culture has been identified as a major factor in cases of financial misconduct, rogue trading, mis-selling, and fraudulent claims practices [42], [43]. A strong risk culture requires ethical leadership, transparent communication, effective whistle-blowing channels, balanced incentive structures, and widespread understanding of risk responsibilities [44], [45]. During the run-up to the financial crisis, many institutions exhibited cultural deficiencies such as excessive risk-taking incentives, normalized rule-bending, and insufficient challenge to executive decisions, leading to internal control failures even when formal controls existed [46].

Information systems and technology represent another critical element of internal control in both banking and insurance. The increasing digitisation of financial operations has brought significant operational efficiencies but also introduced new vulnerabilities. Information systems support control activities such as automated transaction verification, anomaly detection, data accuracy checks, audit trail generation, and risk reporting. However, technology creates risks such as cyberattacks, system outages, data corruption, and unauthorized access. The literature emphasizes the need for strong data governance, integrated system architecture, secure access controls, and real-time monitoring capabilities to maintain internal control effectiveness in technology-enabled environments [47], [48]. Financial institutions must therefore balance the opportunities of technological innovation with robust control systems designed to mitigate technological threats.

Despite decades of research and regulatory attention, challenges persist in implementing effective RBIC systems. Common barriers include lack of coordination between risk management and internal control units, poor data quality, insufficient expertise in risk modelling, outdated information systems, and limited resources for control functions [49], [50]. Many banks and insurers continue to operate with fragmented control structures, siloed departments, and inconsistent risk assessment methodologies. Empirical studies show that internal controls often fail not because they are poorly designed but because they are poorly implemented, misunderstood, or overridden by

management pressure or cultural norms [51], [52]. In some cases, institutions engage in "box-ticking" approaches to control compliance, producing documentation that satisfies regulatory audits but lacks substantive risk-mitigating value [53], [54].

The literature also identifies gaps in the integration of internal control with strategic decision-making. Internal control systems are sometimes viewed as administrative or compliance burdens rather than as tools for enhancing performance and decision quality. Scholars argue that internal control must be embedded within organisational strategy, capital planning, product development, and long-term sustainability frameworks [55], [56]. Without such integration, internal controls remain peripheral and risk becoming detached from the underlying processes they are meant to protect.

Given these challenges, there is a strong theoretical and practical need for conceptual frameworks that integrate governance, risk processes, control design, behaviour, and technology into coherent RBIC models specifically tailored for financial institutions. Existing frameworks provide useful building blocks but are insufficiently sector-specific or lack integrated perspectives that align all major internal control dimensions. The conceptual framework developed in Section 3 responds to this gap by synthesising the literature reviewed here into a comprehensive model designed for application within banking and insurance institutions.

## III. CONCEPTUAL FRAMEWORK FOR RISK-BASED INTERNAL CONTROL IN BANKING AND INSURANCE

The purpose of this section is to present a comprehensive conceptual framework for developing risk-based internal control (RBIC) systems tailored to the banking and insurance sectors. Drawing on literature prior to 2017, the framework integrates insights from internal control theory, enterprise risk management (ERM), governance models, behavioural risk perspectives, sector-specific regulatory doctrines, and information systems research. The framework is built on the premise that internal control in financial institutions must reflect the institution's unique risk profile, regulatory environment, organizational culture, strategic objectives, operational complexity, and technological infrastructure. It posits that RBIC is most effective when structured around five foundational pillars: governance and organizational architecture; risk identification and assessment; risk-based control activities; information, communication, and technology infrastructure; and monitoring and assurance. These pillars are interconnected and mutually reinforcing, forming an integrated internal control environment designed to support resilience, regulatory compliance, and sustainable financial performance.

The conceptual model assumes that effective RBIC is not a static mechanism but a dynamic governance capability. This approach is based on the recognition that risk environments in the banking and insurance sectors evolve continuously due to shifts in market conditions, technological innovation, regulatory expectations, and socio-economic dynamics. Therefore, RBIC systems must be capable of adaptation, learning, and continuous improvement. The framework draws heavily from ERM literature such as COSO's ERM model, which emphasised risk integration, risk appetite alignment, and governance oversight [1], [5]. It also incorporates regulatory doctrines such as Basel II/III and Solvency II, which prescribe governance, risk management, internal control, and reporting standards for banks and insurers, respectively [8]–[15]. While the framework is comprehensive, it remains conceptual and does not prescribe specific operational processes; instead, it articulates the structural, behavioral, and informational conditions under which RBIC can function effectively.

### 3.1 Governance and Organizational Architecture

Governance is the foundation of RBIC. Effective internal control systems originate from the board of directors and senior management, whose decisions establish the tone, structure, culture, and direction of risk management. Literature before 2017 consistently highlights governance failures as root causes of major financial collapses, such as the cases of Lehman Brothers, Northern Rock, and AIG, where boards failed to supervise risk exposures, enforce internal control discipline, or maintain adequate oversight of senior management actions [8], [13]. For this reason, the conceptual framework places governance and

organizational architecture as the first and most influential pillar.

Boards of directors are responsible for defining the institution's risk appetite, approving internal control frameworks, establishing ethical expectations, and overseeing management's execution of risk processes [30], [31]. A risk-based internal control system cannot function without explicit board involvement in risk appetite statements, control strategy approvals, and periodic review of risk exposures. Strong governance requires the board to have dedicated committees such as risk committees and audit committees to supervise specialized aspects of internal control performance. These committees must include members with adequate risk expertise, independence, and experience in financial markets. Research has shown that boards with higher levels of financial literacy and independence tend to enforce stronger internal controls and are less likely to tolerate excessive risk-taking behaviors [32], [33].

Senior management plays a complementary role by translating board directives into operational policies, control structures, and implementation approaches. Management's responsibilities include ensuring adequate staffing, maintaining risk-aware culture, promoting ethical conduct, investing in technology, developing internal control procedures, and coordinating risk functions. Effective RBIC requires management to integrate internal control principles into strategic planning, product development, credit and underwriting decisions, investment policies, and capital allocation. When management is disengaged, inconsistent, or overly focused on short-term profit, internal control systems become symbolic rather than functional, leading to vulnerabilities that can escalate into institutional crises.

The conceptual framework also adopts the three lines of defense (3LoD) model as a structural backbone of internal control governance, consistent with pre-2017 literature [35], [37]. The first line of defense comprises frontline operational units, which are responsible for implementing controls within business processes [57], [58]. The second line consists of risk management and compliance functions, which oversee risk frameworks, analyses risks, and monitor adherence to policies. The third line, internal audit provides independent assurance regarding the adequacy and effectiveness of controls [59], [60]. The conceptual framework emphasizes interdependency among the three lines, noting that communication breakdowns, duplicated responsibilities, or unclear risk ownership often cause internal control failures. Strengthening coordination within the 3LoD structure is therefore a critical aspect of the RBIC model.

Governance also incorporates risk culture the behavioral dimension of internal control. Risk culture refers to the norms, values, behaviors, and attitudes that influence how employees identify, assess, and respond to risk [61], [62]. Studies reveal that even the most sophisticated internal control systems can fail when employees exhibit complacency, excessive risk appetite, unethical behavior, or reluctance to escalate concerns. The conceptual framework therefore places risk culture at the core of governance architecture. Leadership must actively foster a culture that supports transparency, accountability, compliance, and ethical conduct. Incentive structures must discourage opportunistic behavior, encourage adherence to controls, and reward responsible decision-making. Without strong risk culture, RBIC becomes procedural rather than strategic, increasing the risk of misconduct and operational failures.

3.2 Risk Identification and Assessment

The second pillar of the conceptual framework concerns risk identification and assessment of the processes through which an institution recognizes and prioritizes risks. Banking and insurance institutions face diverse risk categories, including credit risk, underwriting risk, market risk, liquidity risk, operational risk, strategic risk, legal risk, cyber risk, and reputational risk. Literature before 2017 underscores that weak risk identification and assessment are major contributors to internal control failures. For example, inadequate credit risk assessment led to widespread loan defaults during the financial crisis, while weak underwriting risk identification contributed to insurer destabilization during catastrophic events [17], [25].

Effective RBIC begins with comprehensive risk identification across organizational levels. This requires institutions to conduct periodic assessments of internal and external factors affecting risk exposure,

including macroeconomic trends, competitor actions, regulatory developments, customer behaviour, technological innovations, and internal process vulnerabilities. Risk identification must be ongoing, dynamic, and forward-looking. Static annual assessments are insufficient for fast-moving financial environments, where risk conditions can change rapidly.

Risk assessment involves evaluating the probability, impact, velocity, and controllability of identified risks. Probability indicates the likelihood of a risk event, while impact refers to the potential financial, operational, regulatory, or reputational consequences. Velocity reflects how quickly a risk materializes, and controllability measures the extent to which an institution can prevent or mitigate the risk. These dimensions are essential because high-impact, high-velocity, and low-controllability risks require strong preventive controls. In contrast, low-impact and slow-velocity risks may require simpler, detection-oriented controls.

The conceptual framework integrates principles from Basel II/III, which require banks to assess credit, market, and operational risks using quantitative models, historical data, and stress-testing techniques [8], [9]. Similarly, Solvency II requires insurers to assess underwriting, reserving, and investment risks using scenario analysis, standard formulas, or internal models [14], [16]. Stress testing and scenario analysis are therefore central risk assessment tools in the RBIC framework. These tools allow institutions to evaluate the resilience of their portfolios, business models, and control systems under extreme but plausible conditions, such as economic downturns, liquidity crises, catastrophic losses, or cyberattacks.

Risk appetite and tolerance thresholds also form part of risk assessment. Risk appetite refers to the level of risk the board is willing to accept, while tolerance establishes operational limits and behavioral boundaries. Effective RBIC requires internal controls to align with the institution's risk appetite. For example, a bank with a low credit risk appetite must enforce stricter credit approval controls, while an insurer with a low underwriting risk appetite must implement tighter pricing and risk selection guidelines. Misalignment between risk appetite and control design leads to inconsistent decision-making and increases exposure to financial loss.

Risk assessment also incorporates data quality, which is crucial for accuracy. Poor data governance undermines risk modelling, reporting, and control monitoring [63], [64]. Literature points to cases in which institutions underestimated risk exposure due to incomplete or inaccurate data, particularly in credit scoring, claims forecasts, and market risk calculations [44], [45], [47]. The conceptual framework therefore emphasizes the need for robust data governance policies to support effective risk identification and assessment.

3.3 Risk-Based Control Activities

Control activities are the most visible component of internal control systems. They refer to the policies, procedures, mechanisms, and actions implemented to prevent, detect, and correct risks. In RBIC, control design depends directly on the outcomes of risk assessment, meaning that controls must be proportional to the level and nature of exposure. This principle aligns with pre-2017 regulatory expectations, which emphasized risk-sensitive control design under Basel III and Solvency II [15]–[20].

Control activities in banking institutions differ from those in insurance due to the unique structure of risks in each sector. In banking, credit risk controls are essential and include borrower verification, collateral valuation, approval hierarchies, credit scoring models, and periodic loan reviews. Weak credit controls contributed significantly to loan losses during the financial crisis. Market risk controls include trading limits, segregation of trading and settlement functions, independent valuation verification, limit monitoring, and VaR analysis [18], [19]. Liquidity risk controls involve monitoring liquidity coverage ratios, maintaining adequate liquid assets, and establishing contingency funding plans. Operational risk controls address process breakdowns, fraud, internal errors, system failures, and external disruptions through approval matrices, reconciliation processes, audit trails, physical security, and cybersecurity layers [20], [23]. Compliance controls, including AML and CTF controls, require customer due diligence, sanctions screening, transaction monitoring, and suspicious activity reporting [22], [23].

In insurance, underwriting controls ensure that risks are selected, priced, and documented correctly. These controls include underwriting guidelines, risk scoring tools, peer review processes, limit authorities, and pricing reviews [24]. Claims management controls require validation of claims, fraud detection mechanisms, loss adjustment verification, and approval hierarchies [25]. Reserving controls focus on actuarial model validation, assumption governance, and data quality controls [26]. Investment controls monitor compliance with investment mandates, diversification limits, valuation policies, and ALM strategies [27]. Reinsurance controls ensure proper risk transfer, counterparty analysis, and treaty compliance [28]. The effectiveness of these controls directly influences an insurer's position of solvency and regulatory compliance [65], [66].

The conceptual framework emphasizes that RBIC must integrate technology-enabled controls. Automation enhances consistency, timeliness, and accuracy of control execution. For example, automated transaction monitoring systems can detect anomalies in real time, while rule-based underwriting engines can ensure adherence to pricing guidelines. However, these tools also require strong access controls, cybersecurity measures, and system governance to mitigate technological risks.

Another key principle of RBIC control design is embedding controls within processes rather than adding them as separate compliance requirements. Embedded controls reduce operational friction, increase efficiency, and improve control adherence. Examples include automated credit scoring integrated into loan origination systems, real-time risk indicators integrated into trading systems, and automated underwriting rules embedded within insurance policy administration systems.

3.4 Information, Communication, and Technology Infrastructure

Information systems form the backbone of modern internal control systems [67], [68]. Financial institutions rely on integrated databases, automated workflows, and advanced analytics to support risk assessment, control execution, and monitoring. Literature highlights that breakdowns in information systems such as poor data quality, lack of integration, limited real-time access, or weak cybersecurity can undermine even the strongest internal control frameworks [69], [70].

The conceptual framework places significant emphasis on information quality [71], [72]. Data must be accurate, complete, consistent, timely, and secure. Banks and insurers require data governance frameworks that standardize data definitions, establish ownership responsibilities, validate data quality, and protect information assets [73], [74]. Given the dependence of risk assessment models on historical and real-time data, data quality directly influences the accuracy of risk forecasts, credit scoring, underwriting decisions, and solvency assessments.

Communication is equally important. RBIC requires seamless communication across organizational levels and departments. Policies, risk alerts, control instructions, compliance requirements, and audit findings must be communicated clearly, consistently, and promptly [75], [76]. Weak communication channels create information asymmetry, delay critical decisions, and limit control effectiveness [77], [78]. Effective RBIC requires reporting dashboards, escalation protocols, cross-departmental coordination, and open communication from frontline staff to senior leaders.

Technology infrastructure enables control automation, real-time monitoring, and independent assurance [79], [80], [81]. Core banking systems, enterprise resource planning (ERP) tools, risk management information systems (RMIS), policy administration systems, and claims management platforms support RBIC by embedding control logic within operational processes [82], [83]. Technology reduces manual errors, increases traceability, enhances transparency, and strengthens oversight. However, technology also introduces new operational risks such as cyber threats, system outages, and data corruption, reinforcing the need for comprehensive IT controls.

3.5 Monitoring, Review, and Assurance

Monitoring is the final pillar of the RBIC conceptual framework. Internal controls must be evaluated continuously to determine their effectiveness, relevance, and alignment with risk appetite. Monitoring activities can be real-time, periodic, or

event-triggered [84], [85]. Literature suggests that institutions with strong monitoring systems detect control failures earlier, respond faster to emerging risks, and maintain higher levels of resilience [86], [87].

The conceptual framework differentiates between management-level monitoring and independent assurance [88], [89]. Management is responsible for ongoing monitoring, including review of key risk indicators (KRIs), control reports, exceptions, and operational deviations. Internal audit provides independent assurance by evaluating control design adequacy, control operating effectiveness, governance processes, and compliance with regulatory requirements [90], [91]. Internal audit must remain independent, objective, and suitably skilled to provide credible assurance. Weak internal audit functions contribute to undetected risks, override management, and regulatory sanctions [92], [93].

Corrective actions and lessons learned complete the monitoring cycle [94], [95]. When deficiencies are identified, institutions must analyse root causes, implement corrective measures, assign accountability, and track remediation [96], [97]. Without effective remediation, monitoring becomes symbolic, and risks remain unaddressed. Strong monitoring reinforces organisational learning and drives continuous improvement in RBIC systems [98], [99], [100].

## IV. DISCUSSION

The purpose of this section is to critically interpret the conceptual framework presented in Section 3 and demonstrate its implications for banking and insurance institutions, regulatory bodies, and the broader field of internal control research. The framework is grounded in well-established pre-2017 scholarship, yet it advances an integrated perspective that bridges theoretical constructs, regulatory expectations, operational realities, and behavioral dynamics. This discussion section positions the framework within the wider discourse on internal control and risk governance, highlighting its value in strengthening organizational resilience, enhancing regulatory alignment, reducing operational vulnerabilities, and improving decision-making quality.

The transition from traditional, compliance-oriented internal control models to risk-based internal control (RBIC) models reflects a fundamental shift in how internal control is conceptualized within financial institutions. In earlier decades, internal control systems tended to focus primarily on procedure adherence, error detection, and fraud prevention. While these remain essential, they do not adequately address the complex, interconnected, and often fast-evolving risks that characterize contemporary banking and insurance operations. The global financial crisis revealed that conventional internal controls were unable to prevent excessive risk taking, mispriced exposures, and flawed decision-making processes. It also highlighted that risks could emerge from areas not traditionally covered by internal control, such as risk culture, governance weaknesses, incentive misalignment, or gaps in risk identification. The conceptual framework developed in this study responds to these limitations by positioning internal control as a central element of risk governance rather than as a peripheral compliance function.

One of the most important contributions of the framework is its emphasis on governance and organizational architecture as the foundation for RBIC. Governance failures have been repeatedly identified in pre-2017 studies as major contributors to control breakdowns, financial misconduct, and institutional collapses. Boards that lack risk expertise or engagement often fail to challenge management decisions or monitor risk exposures effectively. Similarly, management plays a decisive role in operationalizing risk appetite, embedding control activities, and cultivating a risk-aware culture. Without leadership alignment and clear governance structures, even the most technically advanced controls are likely to be overridden, ignored, or poorly implemented. The framework therefore underscores that RBIC must be board-driven, management-enabled, and organizationally embedded, with clear lines of accountability across the three lines of defense.

The integration of risk identification and assessment processes into the internal control environment is also a central advancement of the framework. Internal control in financial institutions cannot be designed in a vacuum; it must be informed by a rigorous

understanding of inherent risks. Banks and insurers face a spectrum of risk exposures credit default, underwriting loss, liquidity stress, market volatility, fraud, regulatory penalties, cyberattacks that must be actively identified, quantified, prioritized, and monitored. Traditional internal control approaches often relied on static risk assessments or rule-based checklists that failed to capture emerging threats. The RBIC framework emphasizes continuous, forward-looking risk assessment supported by stress testing, scenario analysis, and real-time data monitoring. This approach improves the organization's ability to anticipate vulnerabilities rather than merely react to control failures. For example, an insurer using stress scenarios to model catastrophic claims events can design more robust claims validation controls, while a bank conducting liquidity stress tests may implement stronger intraday liquidity controls.

The discussion also highlights that RBIC improves control relevance and efficiency. In traditional internal control models, controls are sometimes applied uniformly across all processes regardless of their risk significance. This results in overcontrolled low-risk areas and under controlled high-risk areas. The RBIC model ensures that resources are allocated proportionately, focusing on the highest sources of risk. This risk-based prioritization is essential in financial institutions where resources for control functions such as internal audit, compliance, and risk management are often constrained. By aligning control intensity with risk exposure, institutions can improve their operational efficiency and reduce unnecessary administrative burdens while maintaining robust risk mitigation.

The conceptual framework's attention to behavioral and cultural dynamics represents another significant contribution. Research before 2017 extensively documented that risk culture influences the success or failure of internal control systems. Weak risk culture contributed to mis-selling scandals, rogue trading episodes, inappropriate underwriting decisions, and fraud in both banking and insurance sectors. These events demonstrated that internal controls are vulnerable to behavioral override when employees lack ethical commitment, when incentives favor excessive risk taking, or when escalation pathways are unclear. By embedding risk culture as a cross-cutting element within governance and across all five pillars, the conceptual framework emphasizes that RBIC is as much a behavioral construct as it is a procedural one. This perspective aligns with leading scholarship in auditing, behavioral governance, and financial risk management, which stresses that internal control effectiveness is contingent on organizational norms, values, and leadership tone.

The inclusion of information, communication, and technology within the conceptual framework responds to the reality that financial institutions increasingly rely on digital systems to execute transactions, store data, assess risks, and implement controls. Information systems have become the nerve center of internal control environments, providing the infrastructure for automated monitoring, workflow management, anomaly detection, and audit trails. However, as literature before 2017 observed, technology also introduces risks such as cybersecurity breaches, system outages, data corruption, and algorithmic bias. The framework balances these dual roles by requiring institutions to strengthen both the technological foundations of control systems and the controls governing technology itself. This includes ensuring data quality, system integration, secure access, and robust IT governance. This discussion thus situates RBIC within the broader trend of digital transformation, recognizing that internal control cannot remain effective without technological advancement.

The monitoring and assurance functions described in the framework are equally essential for RBIC effectiveness. Continuous monitoring allows institutions to track control performance and risk indicators in real time, enabling early detection of deviations or weaknesses. Internal audit provides independent assurance that controls are designed adequately and operate as intended. The conceptual framework positions internal audit as a strategic partner in RBIC, consistent with pre-2017 literature emphasizing the shift toward risk-based auditing. Monitoring and assurance close the feedback loop in internal control, ensuring that controls evolve as risks evolve. This dynamic capability differentiates RBIC from static internal control approaches that may remain unchanged despite shifts in organizational strategy or risk environment.

From a practical perspective, the conceptual framework offers a blueprint that banks and insurers can adapt to their size, complexity, and regulatory environment. A large multinational bank, for example, may operationalize the model with extensive data analytics, automated risk dashboards, and specialized risk committees. A smaller insurance company may apply the same principles using simpler risk matrices, manual review processes, and periodic board reporting. The strength of the framework lies in its scalability and its ability to align with different business models and resource capacities. The model also has significant implications for regulatory compliance. Basel III and Solvency II both require risk-sensitive internal control systems, and the framework provides an integrated interpretation of how institutions can meet these expectations through governance, risk assessment, control design, information systems, and monitoring.

The discussion further acknowledges implementation challenges. Many institutions face organizational silos, limited data integration, inconsistent risk terminology, and resistance to cultural change. Implementing RBIC requires investments in technology, staff training, governance reform, and cross-departmental coordination. Institutions must also recognize that RBIC is an ongoing process rather than a one-time project. Sustaining RBIC requires continuous leadership commitment, periodic reassessment, and adaptation to emerging risks such as cyber threats, regulatory changes, and economic shocks.

From a theoretical standpoint, the conceptual framework contributes to academic literature by integrating elements of internal control, ERM, governance theory, behavioral risk, and technology risk into a unified model specifically tailored for financial institutions. Existing frameworks such as COSO, ISO 31000, and Basel III provide important conceptual components but lack the integrated and sector-specific orientation needed for practical RBIC development. The framework in this study addresses this gap by synthesizing these diverse strands of literature into a coherent structure that captures the interdependence among risk processes, control activities, and organizational behaviors.

Finally, the conceptual framework has implications for future research. Scholars may empirically test the model in banking and insurance environments, evaluate its predictive power in relation to operational losses or regulatory findings, and explore how different organizational factors influence RBIC maturity. Research could also examine the role of emerging technologies such as machine learning, artificial intelligence, or blockchain in strengthening RBIC, provided that such studies use pre-2018 technological contexts. Additionally, cross-country comparisons could reveal how regulatory environments and cultural factors shape RBIC implementation across different jurisdictions.

In conclusion, Section 4 demonstrates that the conceptual framework offers theoretical depth, practical relevance, and regulatory alignment. It advances discourse on internal control by positioning RBIC as an integrated governance capability embedded within the strategy, structure, processes, culture, and information systems of financial institutions. By doing so, the framework provides a strong foundation for the development of more resilient, accountable, and risk-aware banking and insurance organizations.

## CONCLUSION

This paper set out to develop a comprehensive conceptual framework for risk-based internal control (RBIC) tailored to the unique operational and regulatory environments of the insurance and banking sectors. Drawing exclusively from literature and regulatory doctrine published before 2017, the study has demonstrated that traditional, compliance-centric internal control systems are no longer sufficient to manage the complex and interconnected risks faced by contemporary financial institutions. As the introduction and literature review highlighted, financial crises, corporate failures, mis-selling scandals, credit market disruptions, and underwriting collapses have repeatedly exposed the inadequacies of internal controls that fail to incorporate risk sensitivity, governance rigor, behavioral discipline, and technological integration. These historical lessons underscore the necessity of moving internal control beyond checklist compliance toward a holistic governance capacity embedded within the strategic,

operational, informational, and cultural fabric of financial institutions.

The conceptual framework developed in this study synthesizes insights from internal control theory, enterprise risk management, organizational governance, behavioral science, financial regulation, and information systems research into five interdependent pillars: governance and organizational architecture; risk identification and assessment; risk-based control activities; information, communication, and technology infrastructure; and monitoring, review, and assurance. By articulating how these pillars interact dynamically, the framework presents RBIC as an integrated system rather than a collection of isolated controls or departmental responsibilities. Governance establishes the strategic foundation through risk appetite, ethical leadership, board oversight, and the three lines of defense model. Risk identification and assessment ensure that controls are grounded in accurate and forward-looking evaluations of the institution's exposure to credit, underwriting, market, operational, compliance, liquidity, and technological risks. Risk-based control activities translate these assessments into proportionate and context-sensitive interventions embedded within business processes. Information and communication systems provide the technological platform for automation, data governance, real-time monitoring, and cross-functional coordination. Monitoring and assurance close the loop through continuous evaluation, independent review, and corrective action.

A central insight of the framework is that RBIC effectiveness depends as much on organizational culture and behavioral alignment as on technical design. The literature reviewed shows that many internal control failures originate not from the absence of procedures but from weak risk culture, poor communication, misaligned incentive structures, and management override. Consequently, the framework emphasizes risk culture as a cross-cutting element that shapes how control principles are internalized and executed by employees at all levels. By integrating behavioral considerations with structural and procedural elements, the framework provides a more realistic and comprehensive foundation for understanding internal control challenges.

The framework also aligns strongly with regulatory expectations under Basel II/III for banks and Solvency II for insurers. Both regulatory regimes call for risk-sensitive capital assessment, governance clarity, internal model validation, independent review functions, and institution-wide integration of risk management practices. The conceptual model operationalizes these requirements by demonstrating how internal control can serve as the procedural mechanism through which institutions achieve compliance, build supervisory credibility, and strengthen financial resilience. In doing so, it offers regulators a structured approach for assessing the adequacy of internal control systems and for guiding institutions toward more robust risk governance.

While the framework is conceptually robust, its practical implementation will require financial institutions to undertake sustained efforts across governance reform, technological investment, staff training, and cultural transformation. Many institutions may face challenges such as limited resources, inadequate data architecture, organizational silos, or resistance to change. These challenges do not diminish the value of the framework; rather, they underscore the need for scalability and adaptability. The proposed RBIC model can be implemented incrementally, beginning with governance strengthening and risk assessment enhancement before progressing to technology-enabled controls and continuous monitoring systems.

From an academic standpoint, the conceptual framework contributes to the literature by integrating previously disparate strands of research into a unified model specifically designed for the financial sector. Existing frameworks such as COSO and ISO 31000 provide generic guidance but do not fully address the regulatory and operational demands of banks and insurers. By synthesizing sector-specific regulatory requirements with governance theory, risk behavior research, and control design principles, this paper fills a notable gap in the literature and sets the foundation for future research. Potential avenues for empirical validation include comparative studies across jurisdictions, analysis of RBIC maturity levels, quantitative evaluation of RBIC's impact on financial performance or operational losses, and longitudinal studies of RBIC implementation over time.

In conclusion, the conceptual framework presented in this study offers a comprehensive, integrated, and theoretically grounded approach to developing risk-based internal control systems in the banking and insurance sectors. It positions RBIC not as a compliance burden but as a strategic governance capability that enhances institutional resilience, regulatory compliance, risk transparency, cultural discipline, and operational excellence. As financial institutions continue to navigate evolving risks, technological disruption, and increasing regulatory scrutiny, the adoption of risk-based internal control frameworks will be essential for safeguarding organizational stability and contributing to the broader stability of the financial system.

REFERENCES


[1] T. Franke and D. zu Knyphausen-Aufsess, "On dominant logic: review and synthesis," *Journal of Business Economics*, vol. 84, no. 1, pp. 27–70, Jan. 2014, doi: 10.1007/S11573-013-0690-4.

[2] B. Boyce, "Emerging Technology and the Health Insurance Portability and Accountability Act," *J Acad Nutr Diet*, vol. 117, no. 4, pp. 517–518, Apr. 2017, doi: 10.1016/j.jand.2016.05.013.

[3] A. S. Moriya, W. B. Vogt, and M. Gaynor, "Hospital prices and market structure in the hospital and insurance industries," *Health Econ Policy Law*, vol. 5, no. 4, pp. 459–479, Oct. 2010, doi: 10.1017/S1744133110000083.

[4] A. C. T. Smith, F. Sutherland, and D. H. Gilbert, "Changing Forms of Organizing," *Reinventing Innovation*, pp. 19–33, 2017, doi: 10.1007/978-3-319-57213-0_2.

[5] E. Heo, J. Kim, and S. Cho, "Selecting hydrogen production methods using fuzzy analytic hierarchy process with opportunities, costs, and risks," *Int J Hydrogen Energy*, vol. 37, no. 23, pp. 17655–17662, Dec. 2012, doi: 10.1016/j.ijhydene.2012.09.055.

[6] T. Aven, "Risk assessment and risk management: Review of recent advances on their foundation," *Eur J Oper Res*, vol. 253, no. 1, pp. 1–13, Aug. 2016, doi: 10.1016/j.ejor.2015.12.023.

[7] R. R. Sinkovics and A. S. Roath, "Cultivating learning and fostering flexibility in international distribution," *der markt*, vol. 51, no. 1, pp. 3–12, Mar. 2012, doi: 10.1007/S12642-011-0067-6.

[8] F. Aqlan and S. S. Lam, "Supply chain risk modelling and mitigation," *Int J Prod Res*, vol. 53, no. 18, pp. 5640–5656, Sep. 2015, doi: 10.1080/00207543.2015.1047975.

[9] B. B. Schlegelmilch and S. Ram, "The impact of organizational and environmental variables on strategic market orientation: An empirical investigation," *Journal of Global Marketing*, vol. 13, no. 3, pp. 111–127, 2000, doi: 10.1300/J042V13N03_06.

[10] K. Foerstl, C. Reuter, E. Hartmann, and C. Blome, "Managing supplier sustainability risks in a dynamically changing environment-Sustainable supplier management in the chemical industry," *Journal of Purchasing and Supply Management*, vol. 16, no. 2, pp. 118–130, Jun. 2010, doi: 10.1016/j.pursup.2010.03.011.

[11] F. Graetz, "Strategic change leadership," *Management Decision*, vol. 38, no. 8, pp. 550–564, Oct. 2000, doi: 10.1108/00251740010378282.

[12] A. C. T. Smith, F. Sutherland, and D. H. Gilbert, "The Innovation Imperative," *Reinventing Innovation*, pp. 1–17, 2017, doi: 10.1007/978-3-319-57213-0_1.

[13] D. O. Ulrich and N. Smallwood, "Intangibles and Stock Prices: How Leaders Build Market Value," *Investor Marketing*, pp. 261–277, 2003, doi: 10.1007/978-3-322-90350-1_20.

[14] A. Zafer Acar and C. Zehir, "Development and validation of a multidimensional business capabilities measurement instrument," *Journal of Transnational Management*, vol. 14, no. 3, pp. 215–240, 2009, doi: 10.1080/15475770903127050.

[15] C. Bart and A. Pujari, "The performance impact of content and process in product innovation charters," *Journal of Product Innovation Management*, vol. 24, no. 1, pp. 3–19, Jan. 2007, doi: 10.1111/J.1540-5885.2006.00229.X.

[16] O. Khan and B. Burnes, "Risk and supply chain management: Creating a research agenda," *The International Journal of Logistics Management*, vol. 18, no. 2, pp. 197–216, Aug. 2007, doi: 10.1108/09574090710816931.

[17] A. Lopez-Cabrales, R. Valle, and I. Herrero, "The contribution of core employees to organizational capabilities and efficiency," *Hum Resour Manage*, vol. 45, no. 1, pp. 81–109, Mar. 2006, doi: 10.1002/HRM.20094.

[18] S. L. Margolis and C. D. Hansen, "Visions to Guide Performance: A Typology of Multiple Future Organizational Images," *Performance Improvement Quarterly*, vol. 16, no. 4, pp. 40–58, Oct. 2008, doi: 10.1111/J.1937-8327.2003.TB00293.X.

[19] T. Wang, D. Libaers, and H. Jiao, "Opening the Black Box of Upper Echelons in China: TMT Attributes and Strategic Flexibility," *Journal of Product Innovation Management*, vol. 32, no. 5, pp. 685–703, Sep. 2015, doi: 10.1111/JPIM.12152.

[20] T. Biedenbach, "The power of combinative capabilities: Facilitating the outcome of frequent innovation in pharmaceutical R&D projects," *Project Management Journal*, vol. 42, no. 2, pp. 63–80, Mar. 2011, doi: 10.1002/PMJ.

[21] A. Z. Acar and C. Zehir, "The harmonized effects of generic strategies and business capabilities on business performance," *Journal of Business Economics and Management*, vol. 11, no. 4, pp. 689–711, 2010, doi: 10.3846/JBEM.2010.34.

[22] S. J. Grawe, P. J. Daugherty, and A. S. Roath, "Knowledge synthesis and innovative logistics processes: Enhancing operational flexibility and performance," *Journal of Business Logistics*, vol. 32, no. 1, pp. 69–80, Mar. 2011, doi: 10.1111/J.2158-1592.2011.01006.X.

[23] G. Khoshsima, "A strategic model for measuring agility with fuzzy logic," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5370 LNCS, pp. 258–268, 2008, doi: 10.1007/978-3-540-92137-0_29.

[24] V. Paramsothy, P. Woods, and M. Raman, "Success factors for implementation of entrepreneurial knowledge management in Malaysian banks," *Journal of Information and Knowledge Management*, vol. 12, no. 2, Jun. 2013, doi: 10.1142/S0219649213500159.

[25] D. Ulrich and M. F. Wiersema, "Gaining Strategic and Organizational Capability in a Turbulent Business Environment," *https://doi.org/10.5465/ame.1989.4274761*, vol. 3, no. 2, pp. 115–122, May 1989, doi: 10.5465/AME.1989.4274761.

[26] R. Bechtel, "Calculating human capital: The market based valuation of the human resource," *Zeitschrift fur Personalforschung*, vol. 21, no. 3, pp. 206–231, 2007, doi: 10.1177/239700220702100302.

[27] A. Srivastava, "Do CEOs possess any extraordinary ability? Can those abilities justify large CEO pay?," *Asia-Pacific Journal of Accounting and Economics*, vol. 20, no. 4, pp. 349–384, Dec. 2013, doi: 10.1080/16081625.2013.828670.

[28] T. J. Fiksel, Joseph; Polyviou, M; Croxton, K.L; Pettit, "Creating businesses that adapt and flourish in a changing world," *MIT Sloan Manag Rev*, vol. 56, no. 2, pp. 79–86, 2015, Accessed: Sep. 19, 2014. [Online]. Available: https://books.google.com/books/about/Resilient_by_Design.html?id=GAWICgAAQBAJ

[29] W. R. . Gray, J. R. . Vogel, and D. P. . Foulke, "DIY financial advisor : a simple solution to build and protect your wealth," 2015, Accessed: Sep. 18, 2014. [Online]. Available: https://books.google.com/books/about/DIY_Financial_Advisor.html?id=_0tICgAAQBAJ

[30] J. Chen, A. S. Sohal, and D. I. Prajogo, "Supply chain operational risk mitigation: A collaborative approach," *Int J Prod Res*, vol. 51, no. 7, pp. 2186–2199, Apr. 2013, doi: 10.1080/00207543.2012.727490.

[31] A. Ghadge, S. Dani, and R. Kalawsky, "Supply chain risk management: Present and future scope," *The International Journal of Logistics Management*, vol.

23, no. 3, pp. 313–339, Nov. 2012, doi: 10.1108/09574091211289200.

[32] M. Giannakis and T. Papadopoulos, "Supply chain sustainability: A risk management approach," *Int J Prod Econ*, vol. 171, pp. 455–470, Jan. 2016, doi: 10.1016/j.ijpe.2015.06.032.

[33] V. Cho, "A study of the roles of trusts and risks in information-oriented online legal services using an integrated model," *Inf. Manag.*, vol. 43, no. 4, pp. 502–520, Jun. 2006, doi: 10.1016/j.im.2005.12.002.

[34] W. K. K. Hsu, S. H. S. Huang, and W. J. Tseng, "Evaluating the risk of operational safety for dangerous goods in airfreights – A revised risk matrix based on fuzzy AHP," *Transp Res D Transp Environ*, vol. 48, pp. 235–247, Oct. 2016, doi: 10.1016/j.trd.2016.08.018.

[35] S. H. Chung, H. L. Ma, and H. K. Chan, "Cascading Delay Risk of Airline Workforce Deployments with Crew Pairing and Schedule Optimization," *Risk Analysis*, vol. 37, no. 8, pp. 1443–1458, Aug. 2017, doi: 10.1111/RISA.12746.

[36] H. Soleimani, M. Seyyed-Esfahani, and G. Kannan, "Incorporating risk measures in closed-loop supply chain network design," *Int J Prod Res*, vol. 52, no. 6, pp. 1843–1867, Mar. 2014, doi: 10.1080/00207543.2013.849823.

[37] M. G. Goldstein, E. P. Whitlock, and J. DePue, "Multiple behavioral risk factor interventions in primary care. Summary of research evidence," *Am J Prev Med*, vol. 27, no. 2 Suppl, pp. 61–79, 2004, doi: 10.1016/j.amepre.2004.04.023.

[38] P. Luo, H. Wang, and Z. Yang, "Investment and financing for SMEs with a partial guarantee and jump risk," *Eur J Oper Res*, vol. 249, no. 3, pp. 1161–1168, Mar. 2016, doi: 10.1016/J.EJOR.2015.09.032.

[39] I. Heckmann, T. Comes, and S. Nickel, "A critical review on supply chain risk - Definition, measure and modeling," *Omega (United Kingdom)*, vol. 52, pp. 119–132, Apr. 2015, doi: 10.1016/J.OMEGA.2014.10.004.

[40] T. Wang, K. N. Kannan, and J. R. Ulmer, "The association between the disclosure and the realization of information security risk factors," *Information Systems Research*, vol. 24, no. 2, pp. 201–218, 2013, doi: 10.1287/ISRE.1120.0437.

[41] P. Friele, M. Jakob, and J. Clague, "Hazard and risk from large landslides from Mount Meager volcano, British Columbia, Canada," *Georisk*, vol. 2, no. 1, pp. 48–64, Mar. 2008, doi: 10.1080/17499510801958711.

[42] S. K. Mangla, P. Kumar, and M. K. Barua, "Risk analysis in green supply chain using fuzzy AHP approach: A case study," *Resour Conserv Recycl*, vol. 104, pp. 375–390, Nov. 2015, doi: 10.1016/j.resconrec.2015.01.001.

[43] F. G. Cordeiro, B. S. Bezerra, A. S. P. Peixoto, and R. A. R. Ramos, "Methodological aspects for modeling the environmental risk of transporting hazardous materials by road," *Transp Res D Transp Environ*, vol. 44, pp. 105–121, May 2016, doi: 10.1016/j.trd.2016.02.008.

[44] R. Rajesh, V. Ravi, and R. Venkata Rao, "Selection of risk mitigation strategy in electronic supply chains using grey theory and digraph-matrix approaches," *Int J Prod Res*, vol. 53, no. 1, pp. 238–257, Jan. 2015, doi: 10.1080/00207543.2014.948579.

[45] S. V. Scott, J. Van Reenen, and M. Zachariadis, "The long-term effect of digital innovation on bank performance: An empirical study of SWIFT adoption in financial services," *Res Policy*, vol. 46, no. 5, pp. 984–1004, Jun. 2017, doi: 10.1016/J.RESPOL.2017.03.010.

[46] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," *New Economic Windows*, pp. 239–278, 2016, doi: 10.1007/978-3-319-42448-4_13.

[47] S. C. Bankes, "Agent-based modeling: A revolution?," *Proc Natl Acad Sci U S A*, vol. 99, no. SUPPL. 3, pp. 7199–7200, May 2002, doi: 10.1073/PNAS.072081299.

[48] I. Hasan, K. Jackowicz, O. Kowalewski, and Ł. Kozłowski, "Do local banking market structures matter for SME financing and performance? New

evidence from an emerging economy," *J Bank Financ*, vol. 79, pp. 142–158, Jun. 2017, doi: 10.1016/J.JBANKFIN.2017.03.009.

[49] H. Sohn, "Racial and Ethnic Disparities in Health Insurance Coverage: Dynamics of Gaining and Losing Coverage Over the Life-Course," *Popul Res Policy Rev*, vol. 36, no. 2, pp. 181–201, Apr. 2017, doi: 10.1007/S11113-016-9416-Y.

[50] L. Dafny, M. Duggan, and S. Ramanarayanan, "Paying a premium on your premium? Consolidation in the US health insurance industry," *American Economic Review*, vol. 102, no. 2, pp. 1161–1185, 2012, doi: 10.1257/AER.102.2.1161.

[51] L. Dafny, J. Gruber, and C. Ody, "More Insurers Lower Premiums: Evidence from Initial Pricing in the Health Insurance Marketplaces," *Am J Health Econ*, vol. 1, no. 1, pp. 53–81, Jan. 2015, doi: 10.1162/AJHE_A_00003<SPAN.

[52] P. Karaca-Mandic, A. B. Jena, and J. S. Ross, "Health and health care use among individuals at risk to lose health insurance with repeal of the affordable care act," *JAMA Intern Med*, vol. 177, no. 4, pp. 590–593, Apr. 2017, doi: 10.1001/JAMAINTERNMED.2016.9541.

[53] S. F. Shih, C. Y. Lew-Ting, H. Y. Chang, and K. N. Kuo, "Insurance covered and non-covered complementary and alternative medicine utilisation among adults in Taiwan," *Soc Sci Med*, vol. 67, no. 7, pp. 1183–1189, Oct. 2008, doi: 10.1016/J.SOCSCIMED.2008.06.011.

[54] L. Dafny, J. Gruber, and C. Ody, "More insurers lower premiums: Evidence from initial pricing in the health insurance marketplaces," *Am J Health Econ*, vol. 1, no. 1, pp. 53–81, 2015, doi: 10.1162/AJHE_A_00003.

[55] S. Mullainathan, J. Schwartzstein, and W. J. Congdon, "A reduced-form approach to behavioral public finance," *Annu Rev Econom*, vol. 4, pp. 511–540, Jul. 2012, doi: 10.1146/ANNUREV-ECONOMICS-111809-125033.

[56] W. K. T. Cho and B. J. Gaines, "Breaking the (Benford) law: Statistical fraud detection in campaign finance," *American Statistician*, vol. 61, no. 3, pp. 218–223, Aug. 2007, doi: 10.1198/000313007X223496.

[57] M. Brandenburg, K. Govindan, J. Sarkis, and S. Seuring, "Quantitative models for sustainable supply chain management: Developments and directions," *Eur J Oper Res*, vol. 233, no. 2, pp. 299–312, Mar. 2014, doi: 10.1016/j.ejor.2013.09.032.

[58] J. V. Terza, A. Basu, and P. J. Rathouz, "Two-stage residual inclusion estimation: Addressing endogeneity in health econometric modeling," *J Health Econ*, vol. 27, no. 3, pp. 531–543, May 2008, doi: 10.1016/J.JHEALECO.2007.09.009.

[59] G. Y. Song, Y. Cheon, K. Lee, H. Lim, K. Y. Chung, and H. C. Rim, "Multiple categorizations of products: Cognitive modeling of customers through social media data mining," *Pers Ubiquitous Comput*, vol. 18, no. 6, pp. 1387–1403, 2014, doi: 10.1007/S00779-013-0740-5.

[60] E. Demir, Y. Huang, S. Scholts, and T. Van Woensel, "A selected review on the negative externalities of the freight transportation: Modeling and pricing," *Transp Res E Logist Transp Rev*, vol. 77, pp. 95–114, May 2015, doi: 10.1016/j.tre.2015.02.020.

[61] B. Fahimnia, C. S. Tang, H. Davarzani, and J. Sarkis, "Quantitative models for managing supply chain risks: A review," *Eur J Oper Res*, vol. 247, no. 1, pp. 1–15, Nov. 2015, doi: 10.1016/j.ejor.2015.04.034.

[62] L. Tesfatsion, "Agent-based computational economics: Modeling economies as complex adaptive systems," *Inf Sci (N Y)*, vol. 149, no. 4, pp. 262–268, 2003, doi: 10.1016/S0020-0255(02)00280-3.

[63] G. Prause, "Sustainable business models and structures for industry 4.0," *Journal of Security and Sustainability Issues*, vol. 5, no. 2, pp. 159–169, 2015, doi: 10.9770/JSSI.2015.5.2(3).

[64] F. Caccioli, P. Barucca, and T. Kobayashi, "Network Models of Financial Systemic Risk: A Review," *SSRN Electronic Journal*, Nov. 2017, doi: 10.2139/SSRN.3066722.

[65] G. Sanchez, "PLS Path Modeling with R," 2013, *Trowchez Editions*.

[66] J. S. Ringel, C. Eibner, F. Girosi, A. Cordova, and E. A. McGlynn, "Modeling health care policy alternatives," *Health Serv Res*, vol. 45, no. 5 PART 2, pp. 1541–1558, Oct. 2010, doi: 10.1111/J.1475-6773.2010.01146.X.

[67] H. C. Kimaro, "Strategies for Developing Human Resource Capacity to Support Sustainability of ICT Based Health Information Systems: A Case Study from Tanzania," *Electronic Journal of Information Systems in Developing Countries*, vol. 26, no. 1, pp. 1–23, Aug. 2006, doi: 10.1002/J.1681-4835.2006.TB00171.X.

[68] A. Majchrzak, M. L. Markus, and J. Wareham, "Designing for Digital Transformation: Lessons for Information Systems Research from the Study of ICT and Societal Challenges," *MIS Quarterly*, vol. 40, no. 2, pp. 267–277, Feb. 2016, doi: 10.25300/MISQ/2016/40:2.03.

[69] G. Bloom, E. Berdou, H. Standing, Z. Guo, and A. Labrique, "ICTs and the challenge of health system transition in low and middle-income countries," *Global Health*, vol. 13, no. 1, Aug. 2017, doi: 10.1186/S12992-017-0276-Y.

[70] S. Aral, E. Brynjolfsson, and M. Van Alstyne, "Information, technology and information worker productivity task level evidence," *Inf. Syst. Res.*, vol. 23, no. 3, part 2, pp. 849–867, 2012, doi: 10.1287/isre.1110.0408.

[71] P. C. Tetlock, "Information transmission in finance," *Annual Review of Financial Economics*, vol. 6, pp. 365–384, Dec. 2014, doi: 10.1146/ANNUREV-FINANCIAL-110613-034449.

[72] K. Han, Y. Chang, and J. Hahn, "Information technology spillover and productivity: The role of information technology intensity and competition," *J. Manag. Inf. Syst.*, vol. 28, no. 1, pp. 115–145, Jul. 2011, doi: 10.2753/mis0742-1222280105.

[73] P. E. Mbondji, D. Kebede, E. W. Soumbey-Alley, C. Zielinski, W. Kouvividila, and P. S. Lusamba-Dikassa, "Health information systems in Africa: Descriptive analysis of data sources, information products and health statistics," *J R Soc Med*, vol. 107, pp. 34–45, 2014, doi: 10.1177/0141076814531750.

[74] W. F. Boh and D. Yellin, "Using enterprise architecture standards in managing information technology," *Journal of Management Information Systems*, vol. 23, no. 3, pp. 163–207, Dec. 2006, doi: 10.2753/MIS0742-1222230307.

[75] M. Å. Hugoson, "Centralized versus Decentralized Information Systems: A Historical Flashback," *IFIP Adv Inf Commun Technol*, vol. 303, pp. 106–115, 2008, doi: 10.1007/978-3-642-03757-3_11.

[76] R. Koppel, "Great promises of healthcare information technology deliver less," *Healthcare Information Management Systems: Cases, Strategies, and Solutions: Fourth Edition*, pp. 101–125, Sep. 2015, doi: 10.1007/978-3-319-20765-0_6.

[77] P. L. Reichertz, "Hospital information systems - Past, present, future," *Int J Med Inform*, vol. 75, no. 3-4 SPEC. ISS., pp. 282–299, Mar. 2006, doi: 10.1016/J.IJMEDINF.2005.10.001.

[78] S. Madon, S. Krishna, and E. Michael, "Health information systems, decentralisation and democratic accountability," *Public Administration and Development*, vol. 30, no. 4, pp. 247–260, Oct. 2010, doi: 10.1002/PAD.571.

[79] R. Snyder-Halpern, "Indicators of organizational readiness for clinical information technology/systems innovation: A Delphi study," *Int J Med Inform*, vol. 63, no. 3, pp. 179–204, 2001, doi: 10.1016/S1386-5056(01)00179-4.

[80] M. B. Buntin, M. F. Burke, M. C. Hoaglin, and D. Blumenthal, "The benefits of health information technology: a review of the recent literature shows predominantly positive results," *Health Aff*, vol. 30, no. 3, pp. 464–71, Mar. 2011, doi: 10.1377/hlthaff.2011.0178.

[81] M. Mitchell, M. Getchell, M. Nkaka, D. Msellemu, J. Van Esch, and B. Hedt-Gauthier, "Perceived improvement in integrated management of childhood illness implementation through use of mobile technology: Qualitative evidence from a pilot study in Tanzania," *J Health Commun*, vol. 17, no. SUPPL. 1, pp. 118–127, May 2012, doi: 10.1080/10810730.2011.649105.

[82] L. Urquhart and T. Rodden, "New directions in information technology law: learning from human–computer interaction," *International Review of Law, Computers and Technology*, vol. 31, no. 2, pp. 150–169, May 2017, doi: 10.1080/13600869.2017.1298501.

[83] J. Abelson *et al.*, "PUBLIC and PATIENT INVOLVEMENT in HEALTH TECHNOLOGY ASSESSMENT: A FRAMEWORK for ACTION," *Int J Technol Assess Health Care*, vol. 32, no. 4, pp. 256–264, 2016, doi: 10.1017/S0266462316000362.

[84] Z. Mei and Y. Zirong, "Design of epidemic monitoring platform based on ArcGIS," *Proceedings - 14th International Symposium on Distributed Computing and Applications for Business, Engineering and Science, DCABES 2015*, pp. 380–383, Mar. 2016, doi: 10.1109/DCABES.2015.102.

[85] "Harmonized monitoring and evaluation indicators for procurement and supply management systems," 2011, *World Health Organisation*.

[86] K. Singh, P. J. Best, M. Bojilov, and C. Blunt, "Continuous Auditing and Continuous Monitoring in ERP Environments: Case Studies of Application Implementations," *Journal of Information Systems*, vol. 28, no. 1, pp. 287–310, Jun. 2014, doi: 10.2308/ISYS-50679.

[87] W. Eckerson, "Characteristics Of Effective Performance Metrics," *Performance Dashboards: Measuring, Monitoring And Managing Your Business*, p. 209 pp., 2011, Accessed: Sep. 15, 2014. [Online]. Available: https://books.google.com/books/about/Performance_Dashboards.html?id=5nuYDwAAQBAJ

[88] C. for M. and M. Services, "Quality Assurance and performance improvement."

[89] J. Dai and M. A. Vasarhelyi, "Toward Blockchain-Based Accounting and Assurance," *Journal of Information Systems*, vol. 31, no. 3, pp. 5–21, Sep. 2017, doi: 10.2308/ISYS-51804.

[90] A. Hudic *et al.*, "A multi-layer and multitenant cloud assurance evaluation methodology," *Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom*, vol. 2015-February, no. February, pp. 386–393, Feb. 2015, doi: 10.1109/CLOUDCOM.2014.85.

[91] K. Pollard, A. L. Donskoy, P. Moule, C. Donald, M. Lima, and C. Rice, "Developing and evaluating guidelines for patient and public involvement (PPI) in research," *Int J Health Care Qual Assur*, vol. 28, no. 2, pp. 141–155, Mar. 2015, doi: 10.1108/IJHCQA-01-2014-0001.

[92] M. K. Power, "Auditing and the production of legitimacy," *Account Organ Soc*, vol. 28, no. 4, pp. 379–94, 2003, doi: 10.1016/s0361-3682(01)00047-2.

[93] E. A. Gordon, E. Henry, T. J. Louwers, and B. J. Reed, "Auditing Related Party Transactions: A Literature Overview and Research Synthesis," *Accounting Horizons*, vol. 21, no. 1, pp. 81–102, Mar. 2007, doi: 10.2308/ACCH.2007.21.1.81.

[94] T. Greenhalgh and R. Peacock, "Effectiveness and efficiency of search methods in systematic reviews of complex evidence: Audit of primary sources," *Br Med J*, vol. 331, no. 7524, pp. 1064–1065, Nov. 2005, doi: 10.1136/BMJ.38636.593461.68.

[95] M. J. Nigrini, "Benford's law: Applications for forensic accounting, auditing, and fraud detection," *Benford's Law: Applications for Forensic Accounting, Auditing, and Fraud Detection*, pp. 1–330, Jan. 2012, doi: 10.1002/9781119203094.

[96] D. J. Teece, "Business models, business strategy and innovation," *Long Range Plann*, vol. 43, no. 2–3, pp. 172–194, Apr. 2010, doi: 10.1016/J.LRP.2009.07.003.

[97] K. Katircioglu *et al.*, "Supply chain scenario modeler: A holistic executive decision support solution," *Interfaces (Providence)*, vol. 44, no. 1, pp. 85–104, Jan. 2014, doi: 10.1287/INTE.2013.0725.

[98] B. A. Lameijer, J. De Mast, and R. J. M. M. Does, "Lean six sigma deployment and maturity models: A critical review," *Quality Management Journal*, vol. 24, no. 4, pp. 6–20, 2017, doi: 10.1080/10686967.2017.12088376.

[99] L. Belone *et al.*, "Community-Based Participatory Research Conceptual Model: Community Partner Consultation and Face Validity," *Qual Health Res*,

vol. 26, no. 1, pp. 117–135, Jan. 2016, doi: 10.1177/1049732314557084.

[100] M. Brandenburg and T. Rebs, “Sustainable supply chain management: A modelling perspective,” *Ann Oper Res*, vol. 229, no. 1, pp. 213–252, Jun. 2015, doi: 10.1007/S10479-015-1853-1.