International Journal of Multidisciplinary Research and Growth Evaluation
ISSN: 2582-7138
Received: 27-11-2021; Accepted: 29-12-2021
www.allmultidisciplinaryjournal.com
Volume 2; Issue 6; November-December 2021; Page No. 896-907

Cross-Border Segregation of Duties and Access Governance in Multinational Treasury: A Conceptual Framework

Elizabeth A Dogbatsey [1], Osemudiamhen Ebhojie [2*], Ajibola Oluwafemi Oyeleye [3]
[1] Weave Ghana Ltd (A subsidiary of Godrej Consumer Products Limited), Ghana
[2] Shell, Lagos, Nigeria
[3] PricewaterhouseCoopers (PwC) Canada, Toronto, Canada

Corresponding Author: **Osemudiamhen Ebhojie**

DOI: https://doi.org/10.54660/.IJMRGE.2021.2.6.896-907

Abstract
Segregation of duties (SoD) and user access governance constitute a foundational layer of internal control in treasury operations, but the cross-border character of multinational treasury complicates their design and operation. Common platforms, regional service centres, and local statutory requirements interact to produce a control environment in which rigid SoD rules developed for single-jurisdiction operations produce material inefficiencies without necessarily reducing risk. This article develops a cross-border SoD and access-governance framework for multinational treasury functions, grounded in the Committee of Sponsoring Organizations of the Treadway Commission (COSO) internal control framework (COSO, 2013), the ISACA Control Objectives for Information and Related Technology (COBIT) framework (ISACA, 2019), and the empirical literature on information-system access controls (Warkentin & Willison, 2009; Hoitash *et al*., 2009). The framework distinguishes three control layers: transactional SoD within the treasury management system, functional SoD across treasury teams, and cross-border SoD between shared-service centres and local treasuries. It identifies the control-objective conflicts that arise between efficiency-maximising and risk-minimising access designs, and proposes a governance architecture for resolving them. The article develops six propositions about the relationship between access-governance maturity and treasury-specific risk outcomes, including unauthorised-payment frequency, reconciliation-break volume, and audit-finding severity. It concludes by identifying research priorities including the effect of emerging identity-governance technologies on SoD enforcement cost, the interaction between Sarbanes-Oxley (SOX) Section 404 testing and cross-border SoD design, and the moderating role of treasury centralisation on access-governance effectiveness.

Keywords: Segregation of duties, Access governance, Multinational treasury, Internal control, COBIT, SOX compliance, Shared-service centres

1. Introduction
Segregation of duties (SoD) is among the oldest and most fundamental principles of internal control in financial operations. At its core, SoD requires that no single individual have the capacity to both initiate and approve a transaction, such that any material transaction involves the cooperation of two or more independent individuals. The principle reduces the probability of unauthorised activity and provides a structural check on fraud and error (COSO, 2013; Turner, 2006). Applied to treasury, SoD is operationalised through the assignment of system access rights: initiation of payments, authorisation of payments, creation of counterparty records, maintenance of hedging limits, and reconciliation of settled transactions must each be performed by different individuals, with supporting system enforcement of the separation.

Access governance is the institutional apparatus that operationalises SoD in multi-user systems. It comprises the policies through which access rights are assigned, the review processes through which rights are periodically re-certified, the technical controls through which access is enforced, and the exception handling through which breaks in SoD are identified and remediated. In single-jurisdiction operations, access governance is conceptually straightforward: a treasury team operates on a single platform, with access rights assigned on a role basis, and SoD is enforced through native platform functionality with periodic internal audit review (IIA, 2020; Wright, 2008). The literature on single-jurisdiction access governance is reasonably well developed and the practitioner guidance mature; the conceptual challenges addressed in this article arise specifically at the cross-border extension

of the single-jurisdiction model.

In multinational treasury, the picture is materially more complex. A single platform, often a centrally hosted treasury management system (TMS), may be accessed by users in multiple jurisdictions, with different statutory requirements for authorisation, different local banking relationships, and different service-level expectations. Regional service centres concentrate processing activity, raising both efficiency and access-concentration risks. Local entities retain specific treasury responsibilities that interact with centralised activity. The resulting access architecture must balance efficiency, risk-management, and local-regulatory considerations, and the balance differs across organisational contexts (Polak, 2009; Polak & Kocurek, 2007).

The empirical literature on access controls has developed primarily in the context of financial reporting controls under the Sarbanes-Oxley Act of 2002 (SOX) (Ashbaugh-Skaife *et al*., 2008; Bhaskar *et al*., 2019; Doyle *et al*., 2007; Hoitash *et al*., 2009; Klamm & Watson, 2009), and has documented the relationship between access-control weaknesses and material weakness findings. The treasury-specific literature is thinner, and is concentrated in practitioner-oriented publications rather than peer-reviewed research. This asymmetry is reflected in the practice, where treasury SoD design is often treated as an operational detail rather than as a control design problem requiring framework-level attention. A parallel theoretical strand, grounded in agency theory (Jensen & Meckling, 1976) and the sociology of auditing (Power, 1997), informs the interpretation of SoD as both an economic and institutional artefact.

This article develops a cross-border SoD and access-governance framework for multinational treasury. The framework distinguishes three control layers: transactional SoD within the TMS, functional SoD across treasury teams, and cross-border SoD between shared-service centres and local treasuries. Each layer is characterised by distinctive risks, distinctive control mechanisms, and distinctive conflicts between efficiency-maximising and risk-minimising access designs. The framework proposes a governance architecture for resolving the conflicts, and generates six propositions about the relationship between access-governance maturity and treasury-specific risk outcomes. The conceptual architecture draws on four complementary literatures — internal control, information systems, multinational treasury organisation, and the empirical evidence on SOX Section 404 access deficiencies — and integrates them through a unified analytical vocabulary that previous treatments have lacked.

The conceptual architecture is summarised in Figure 1. The three layers interact, and weakness at any layer can compromise the control environment as a whole.

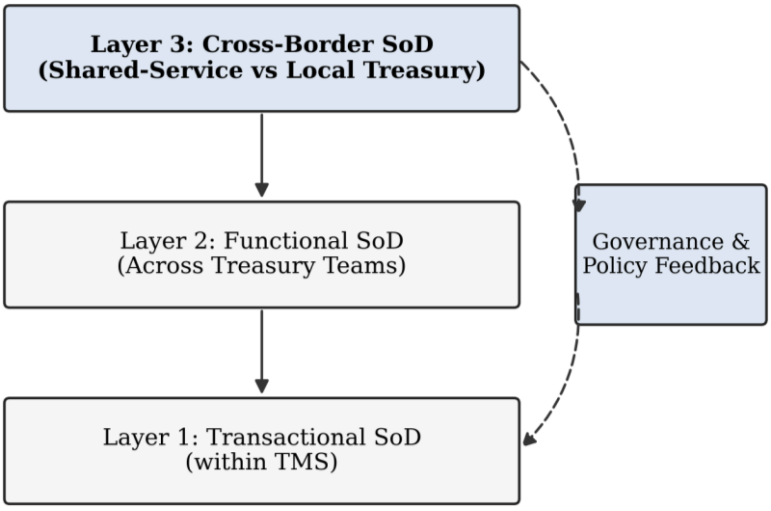

Fig 1: Three layers of cross-border SoD and access governance in multinational treasury. Arrows indicate control dependencies and information flows.

2. Theoretical Foundations

The internal control literature provides the foundation. The COSO Internal Control Integrated Framework identifies segregation of duties as a category of control activity that operates across the five components of internal control (COSO, 2013). The framework does not prescribe specific SoD rules but requires that the organisation identify the incompatible duties relevant to its activities and implement controls to ensure their separation. Applied to treasury, the incompatible duties typically identified are: payment initiation and authorisation; payment authorisation and settlement reconciliation; counterparty master-data maintenance and transaction processing; hedging-limit configuration and hedging-transaction execution.

The COBIT framework provides the information-technology dimension. COBIT specifies access-governance objectives, including identification and authentication, authorisation and access, and monitoring of access (ISACA, 2019). Applied to treasury, the COBIT objectives operationalise SoD through technical access controls in the TMS and associated systems, and through the processes that manage access-right provisioning, re-certification, and deprovisioning. The COBIT framework has achieved widespread adoption in information-systems audit, and its concepts are reflected in the design of most enterprise-grade TMS platforms.

The empirical literature on access-control weakness provides the evidence base for understanding the consequences of poor access governance. Hoitash, Hoitash, and Bedard (2009) documented the relationship between the scope of access-related control weaknesses and the likelihood of material weakness findings under SOX Section 404. Ashbaugh-Skaife, Collins, Kinney, and LaFond (2008) showed that remediation of access-control weaknesses is associated with reduction in abnormal accruals. The literature identifies

access governance as a leading indicator of broader control effectiveness. Parallel work in the information-systems literature has developed models for identity and access management in distributed, federated, and multi-cloud environments that are increasingly relevant to treasury platforms hosted outside the traditional on-premises perimeter (Mbonu *et al*., 2020a; Mbonu *et al*., 2020b; Oshoba *et al*., 2019).

The information-security literature contributes an adjacent perspective. Warkentin and Willison (2009) and Siponen and Vance (2010) examine the behavioural determinants of information-security policy compliance, and their findings generalise to SoD adherence in treasury contexts: where organisational culture supports compliance, access-governance policies are adhered to with limited enforcement; where culture does not support compliance, technical controls must compensate for behavioural gaps. For cross-border treasury operations, cultural variation across jurisdictions adds a distinctive dimension to the behavioural-control-culture interaction.

The multinational treasury literature provides the environmental context. Polak (2009) and subsequent work (Polak & Kocurek, 2007) identify the hub-and-spoke structures that characterise modern multinational treasury, with global treasury centres coordinating policy and providing shared services to regional or local treasuries. The structural evolution of multinational treasury has implications for SoD design that the generic internal control literature does not address, and that the framework developed here specifically attempts to resolve.

A further theoretical strand concerns the governance of controls over information-technology change. Standards-based guidance such as NIST SP 800-53 and the NIST Cybersecurity Framework (NIST, 2018) offers structured references for the maintenance of access controls under continuous technology change, and an emerging body of empirical work examines the application of such frameworks to financial-services and multinational contexts (Chalmers *et al*., 2019). The framework developed here draws on this guidance for the maintenance dimension of access governance.

The auditing and assurance literature adds a further perspective. Materiality, reliance on internal controls, and the testing strategies employed by external auditors shape the effective cost of SoD design decisions for reporting entities. Studies have documented that well-designed access controls reduce the scope of substantive audit work, producing measurable reductions in audit fees and audit effort (Messier *et al*., 2017; Morris, 2011). The auditing dimension therefore imposes an economic discipline on access-governance design that operates alongside the risk-management discipline.

The literature on information-systems control and audit, developed through the work of Weber (1999) and subsequent contributors, provides the technical foundation for the design of access controls in complex system landscapes. This body of work has been increasingly integrated with accounting control theory through contributions such as Turner and Weickgenannt (2013) and Hall (2015), which provide textbook-level syntheses that inform the design of the framework advanced in this article.

The historical evolution of SoD thinking provides useful context. Early conceptions of SoD arose from manual double-entry bookkeeping traditions and from the nineteenth-century development of fiduciary accounting in trust and estate administration. The principle was then codified in the accounting profession's audit guidance during the twentieth century, progressively extended to cover electronic data processing as computerised accounting systems displaced manual ledgers, and eventually integrated into the systems-oriented internal control frameworks that emerged during the 1980s and 1990s (Colbert & Bowen, 1996; Weber, 1999). The contemporary application of SoD in multinational treasury contexts builds on this inherited conceptual apparatus but must adapt it to circumstances its original architects did not anticipate.

A distinct theoretical strand concerns the role of trust in access governance. Trust-based access arrangements, in which access rights are granted to individuals whose competence and integrity are vouched for by their organisational position, have historically been the default in many treasury operations. Rule-based access arrangements, in which access rights are specified in formal policy and enforced through system controls, have progressively displaced trust-based arrangements as treasury operations have grown in scale and complexity. The transition from trust-based to rule-based access is not costless: rule-based access requires investment in policy specification, in system configuration, and in ongoing governance, and it reduces the discretion available to experienced treasury staff (Warkentin & Willison, 2009; Willison & Warkentin, 2013). The framework developed here is grounded in the rule-based tradition but accommodates the practical reality that elements of trust-based governance remain embedded in most treasury operations, particularly at senior levels.

The theoretical framing also draws on the contingency tradition in management control research, which holds that control systems should be designed to match the environmental, organisational, and strategic conditions under which they operate. Applied to SoD and access governance, the contingency perspective implies that the appropriate configuration of controls will vary across organisations with different scale, geographic footprint, regulatory environment, and strategic priorities. The framework developed here is consistent with the contingency perspective: it specifies the dimensions along which configuration decisions must be made rather than prescribing a single configuration that applies to all multinational treasury operations. Configuration decisions are the responsibility of the organisation's governance arrangements, informed by the analytical vocabulary the framework provides (Chapman, 2005; Sutton, 2006).

3. Methodology

The article adopts a conceptual methodology, drawing together insights from the internal control, information-systems, and multinational-treasury literatures to build a framework that addresses a specific organisational problem not adequately treated by any single literature. The conceptual approach is appropriate where the phenomenon is observable but the analytical vocabulary for describing it is fragmented across traditions, and where the contribution sought is the integration of those traditions into a structured framework that supports subsequent empirical work.

The synthesis followed a three-step protocol. First, a structured review of the relevant literatures identified the concepts, theories, and empirical findings bearing on cross-border SoD and access governance. Second, the structural features of multinational treasury operations were

characterised through reference to practitioner sources and to the multinational-treasury literature, producing the three-layer architecture of transactional, functional, and cross-border SoD. Third, the empirical literature on access-control weakness was used to derive testable propositions linking access-governance maturity to treasury-specific outcomes.

The framework is presented as a design theory in the sense of Gregor and Jones (2007): it specifies both the constructs involved in the phenomenon of interest (the three SoD layers, the access-governance mechanisms) and the relationships among them (the propositions). Design theories differ from explanatory theories in that they aim to guide the design of effective interventions, rather than solely to explain observed phenomena. The framework advanced here is therefore intended to support both academic investigation of cross-border SoD and practitioner design of SoD architectures for multinational treasury.

Limitations of the conceptual approach are acknowledged. The framework has not been empirically tested, and subsequent empirical work is required to validate the propositions advanced. The three-layer structure is an analytical abstraction, and real treasury operations may not cleanly fit the three layers in every instance. The framework assumes a multinational treasury context; application to single-jurisdiction or smaller-scale treasury operations would require adaptation. These limitations do not undermine the contribution but define the scope within which the contribution is offered.

The conceptual contribution also interacts with the practitioner literature on treasury transformation. Practitioner guidance from international treasury associations and from advisory firms has increasingly addressed cross-border SoD as a distinct topic, reflecting the operational salience of the issue in current treasury-transformation programmes. The conceptual framework advanced here aims to provide the analytical rigour that such practitioner guidance has typically lacked, and to support subsequent research that bridges the practitioner and academic literatures in a domain where the two communities have developed largely in parallel.

The methodological approach reflects a specific choice about the type of contribution the article aims to make. Rather than producing new empirical evidence about observed practice, the article produces a structured vocabulary that subsequent empirical work can use to measure, classify, and compare observed practice. The choice is justified by the observation that existing empirical work has been hampered by the absence of shared analytical categories, producing evidence that is difficult to synthesise or to generalise across contexts. The conceptual contribution, by supplying those categories, is intended to enable a cumulative empirical programme that would not be feasible without the shared vocabulary. Whether the programme develops depends on whether subsequent researchers find the categories useful, and on whether the propositions advanced generate empirically productive investigation.

4. The Three Layers of SoD

The first layer is transactional SoD within the TMS. This layer comprises the enforcement of separation between incompatible duties at the transaction level: payment initiation versus authorisation, master-data maintenance versus transaction processing, hedging-limit configuration versus hedging-transaction execution. Transactional SoD is operationalised through the role-based access control (RBAC) functionality of the TMS, with roles defined to include sets of incompatible-duty combinations and users assigned to roles consistent with their job responsibilities. The effectiveness of transactional SoD depends on the thoroughness of the role design, the completeness of the SoD rule set, and the quality of ongoing access-certification processes.

Transactional SoD faces several recurring design challenges in multinational treasury. Role proliferation arises when different jurisdictions or different business units require slightly different access configurations, and the result can be a role catalogue so complex that its effective administration becomes impracticable. Role consolidation, in which different access patterns are aggregated into a smaller number of standard roles, addresses proliferation but risks granting access beyond the minimum required by individual users. The design trade-off between role proliferation and role consolidation is a persistent source of tension and requires explicit governance rather than ad-hoc resolution (Bertino & Ferrari, 2018; Ferraiolo *et al*., 2001).

The second layer is functional SoD across treasury teams. This layer comprises the separation of duties between teams responsible for different functional areas of treasury: front-office teams responsible for execution of trades and payment initiation; middle-office teams responsible for policy monitoring, risk analytics, and position reporting; back-office teams responsible for settlement, reconciliation, and accounting. The three-part structure is a standard feature of developed-market treasury and is increasingly adopted in emerging-market treasuries as scale and complexity grow (Polak, 2009).

Functional SoD faces distinct challenges in multinational contexts. Geographic distance between functional teams can erode the day-to-day coordination required for effective SoD operation. Local entities with small treasury teams may not have the headcount to sustain three-part functional separation, requiring hybrid arrangements in which some functional activities are centralised while others remain local. The hybrid arrangements create additional complexity in the design of access rights, because the functional separation operates partly within the local treasury and partly across the local-central interface.

The third layer is cross-border SoD between shared-service centres and local treasuries. This layer addresses the division of responsibilities between a centralised service centre and the local treasury teams that retain specific activities for regulatory, relationship-management, or operational reasons. Cross-border SoD is the most novel of the three layers in analytical terms, and the least addressed by existing literature. It requires the specification of which duties are centralised, which are local, and what access rights are required for each location to perform its assigned duties without overlapping with duties assigned elsewhere.

Cross-border SoD faces the distinctive challenge of reconciling global efficiency with local control effectiveness. A high degree of centralisation produces scale economies but concentrates access rights in the service centre, creating access-concentration risk that requires additional compensating controls. A low degree of centralisation disperses access but reduces scale economies and raises the probability of inconsistent control practice across jurisdictions. The design problem at this layer is not to maximise either dimension but to identify the balance that delivers acceptable control at acceptable cost, and the balance

will differ across organisations based on their size, geographic footprint, and regulatory environment (Nandi & Kumar, 2016; Quattrone & Hopper, 2005).

A specific cross-border challenge concerns the handling of emergency access. When local staff become unavailable due to illness, leave, or turnover, treasury operations must continue, and emergency access arrangements must permit continuity without creating persistent SoD violations. The recurring pattern observed in multinational treasury is that emergency access is granted ad hoc and then not reliably revoked, accumulating into a shadow population of granted-but-unintended access rights. The preventive response is a formal emergency-access protocol with mandatory time limits, explicit approval workflows, and automated revocation at the expiry of the granted period (Canada *et al*., 2009; Rubino & Vitolla, 2014).

The integration of the three layers requires attention to their operational interaction. Transactional SoD operates at microsecond resolution, with access decisions made at each user action. Functional SoD operates at the level of job descriptions and team structures, with access rights aggregated into role definitions that are revised on a multi-month cadence. Cross-border SoD operates at the level of organisational design, with the division of duties between central and local teams reassessed on a multi-year cadence as the treasury function evolves. The three time horizons create coordination challenges that a unified governance framework must explicitly address (Chang *et al*., 2014; Colbert & Bowen, 1996; Debreceny, 2013).

The interaction between the three layers also produces opportunities for reinforcement. A well-designed cross-border architecture simplifies the functional SoD design by reducing the number of duty combinations that must be separated within each team. A disciplined functional SoD design simplifies the transactional SoD rule set by collapsing large numbers of possible access-right combinations into a smaller number of policy-consistent roles. The reinforcement operates in both directions: transactional SoD data (observed access patterns, reconciliation-break patterns) feeds back into the functional and cross-border designs, supporting their iterative refinement. Identification and audit of the interaction patterns is supported by process-mining analytics on TMS event logs, which has been shown to produce auditable evidence of control operation in ERP environments (Jans *et al*., 2014; Kuhn & Sutton, 2010).

A specific consideration at the transactional layer is the handling of inactive or dormant accounts. Over multi-year operations, user accounts accumulate that belong to former employees, to contractors whose engagements have ended, or to system service accounts whose original purpose has been superseded. Without regular review, these dormant accounts represent an access surface that can be exploited without being immediately noticed. Disciplined dormant-account management, with automated detection of accounts inactive beyond defined periods and with mandatory remediation workflows, is a baseline expectation for access governance in mature treasury operations (Bertino & Ferrari, 2018; Hall, 2015).

At the functional layer, the boundary between treasury and the adjacent finance functions (general accounting, accounts payable, accounts receivable, tax) produces a distinct class of SoD considerations. Treasury payments flow into or out of accounts-payable and accounts-receivable ledgers; treasury hedging transactions generate accounting entries requiring general-ledger reflection; treasury tax positions interact with the tax function's reporting responsibilities. Effective functional SoD must therefore extend beyond the internal three-part structure of treasury to cover the interfaces with adjacent functions. The interface-SoD dimension is typically under-addressed in both the practitioner literature and the academic literature, and it represents an area where the framework advanced here could be usefully extended in subsequent work (O'Leary, 2000; Sutton, 2006).

Role-based access control implementation at the transactional layer requires substantial up-front investment in role design, and the quality of the role design strongly influences the subsequent maintainability of the access architecture. Well-designed roles reflect the actual duties performed by users with those roles, are consistent across geographic locations for users performing similar duties, and can be maintained without frequent ad-hoc modifications. Poorly-designed roles proliferate as ad-hoc extensions accumulate to address specific user needs, and eventually become indistinguishable from ungoverned access. The discipline of periodic role-design review, supported by analytics on actual access-use patterns, sustains role-design quality over the multi-year lifetime of the access architecture (Ferraiolo *et al*., 2001; Rubino & Vitolla, 2014).

Cross-border SoD in practice frequently operates under time-zone constraints that are not emphasised in generic internal control literature. Treasury shared-service centres located in one time zone must process transactions initiated in distant time zones, with the time difference producing either compressed processing windows or extended processing cycles depending on the direction of the time offset. Control design must accommodate these time-zone dynamics, with handoff protocols that preserve SoD across the time-zone boundary, with monitoring arrangements that cover the full twenty-four-hour cycle, and with escalation mechanisms that function outside normal business hours in either the centre or the local jurisdiction. Treasury operations in global groups typically operate a follow-the-sun model in which processing responsibility shifts across centres as the working day advances, and the SoD architecture must preserve its integrity across the handoffs that occur at each shift.

The physical security dimension of access governance deserves brief attention. Treasury platforms contain high-value access rights that warrant protection against physical as well as logical compromise. Workstations used for treasury transaction initiation should be located in controlled-access areas; printing of sensitive treasury documents should be restricted to trusted devices; hardware tokens used for strong authentication should be issued and retrieved under defined procedures. Physical security arrangements for treasury are typically less developed than the logical access controls, and a recurring finding in internal audit reviews is that physical security gaps provide compensating-control bypasses for otherwise effective logical controls (Cerullo & Cerullo, 2005; Hall, 2015).

Table 1 summarises the three layers of cross-border SoD, their operational components, and the principal design challenges associated with each layer.

Table 1: Three layers of cross-border SoD, their operational components, and their principal design challenges in multinational treasury.

Layer	Operational components	Principal design challenge
Transactional (within TMS)	RBAC roles, SoD rule enforcement, access certification	Role proliferation versus role consolidation
Functional (across teams)	Front/middle/back office separation	Hybrid arrangements for small local treasuries
Cross-border (SSC vs local)	Division between central and local duties	Efficiency versus concentration risk

5. Risk Categories and the Consequences of Weak Access Governance

Risks arising from weak SoD and access governance in treasury fall into four categories. The first is unauthorised-payment risk. Where the access rights to initiate and authorise payments are not separated, or where the authorisation step can be circumvented through user impersonation or shared credentials, the control that prevents unauthorised external outflows is weakened. The risk is particularly acute in high-volume payment environments, where manual review of all payments is infeasible and controls depend on automated enforcement of SoD at the point of payment release. The adoption of multi-factor authentication and stronger user-identity controls has been shown to reduce the surface area for credential-based impersonation in enterprise payment and messaging environments (Oshoba *et al*., 2021), and integrated cybersecurity and anti-money-laundering architectures have been proposed to extend the preventive control envelope in financial-services settings (Fadayomi *et al*., 2021).

The second is reconciliation-break risk. Where the separation between transaction processing and reconciliation is weak, errors and anomalies introduced into the transaction record can propagate through reconciliation without detection. The downstream consequence is that exception-based monitoring, which depends on reconciliation as its primary input, fails to identify the anomalies at the point at which remediation is cheapest. Reconciliation breaks also interact with audit scope: auditors rely on reconciliations as primary evidence, and high rates of unresolved breaks induce expanded substantive testing that increases audit cost and disruption (Doyle *et al*., 2007; Kinney, 2000).

The third is compliance-drift risk. Access rights, once granted, tend to accumulate over time as users move between roles and as temporary access privileges become permanent. Without disciplined access-certification processes, the granted access population drifts away from the access population consistent with role-based policy, and SoD properties that were present at role design time erode over subsequent operation. The compliance-drift risk is particularly salient in long-running TMS deployments, where successive policy decisions accumulate into an access landscape that no one clearly understands (Chalmers *et al*., 2019; Warkentin & Willison, 2009).

The fourth is audit-finding risk. Control weaknesses identified in SOX Section 404 testing or in statutory audit translate into expanded audit scope, increased testing cost, and in material cases into restatement or disclosure of material weakness. The empirical literature shows a consistent relationship between access-control weakness and audit outcomes (Doyle *et al*., 2007; Hoitash *et al*., 2009). For multinational groups, the reputational and cost implications of material weakness findings are significant.

The four risk categories interact. Weak transactional SoD elevates unauthorised-payment risk directly and elevates reconciliation-break risk through the increased volume of anomalies. Compliance drift raises all four risks, because drift produces an access landscape that is both more vulnerable to unauthorised activity and more difficult to reconcile. Audit-finding risk is a lagging indicator that aggregates the effects of the other three, and its magnitude scales with the size and visibility of the affected entity. The interaction means that access-governance reforms typically produce joint improvements across multiple risk categories, even where the reform is targeted at one.

A fifth risk, less commonly discussed but increasingly material, is cyber-enabled fraud risk. Where access governance is weak, the credentials required to initiate or authorise payments can be obtained by external attackers through phishing, business-email compromise, or credential-stuffing attacks. Once obtained, the credentials permit the attacker to execute the same transactions available to the legitimate user, and the SoD controls that protect against internal fraud can be completely bypassed. The mitigation requires the combination of SoD design with strong authentication (multi-factor, risk-based), with transaction anomaly detection, and with out-of-band verification for high-value or unusual transactions (Benaroch *et al*., 2012; Willison & Warkentin, 2013).

A further risk dimension concerns the interaction between SoD weakness and operational-risk-event accumulation. When reconciliation breaks, policy exceptions, or settlement failures occur more frequently due to SoD weakness, the operational-risk loss register grows, and the capital charge applied to operational risk (under Basel III for financial-services firms, or under analogous frameworks for non-financial firms) increases. The direct financial effect of weak SoD therefore extends beyond the realised losses to the regulatory and capital-adequacy consequences that follow from the pattern of loss events (Cerullo & Cerullo, 2005; Hall, 2015).

The cumulative and compounding character of these interactions deserves emphasis. Individual SoD weaknesses may appear minor when considered in isolation, but their aggregate effect on the control environment can be substantial when the weaknesses accumulate across multiple dimensions. Effective governance therefore requires attention not only to individual control-point weaknesses but also to the patterns of weakness that emerge across the control landscape. Portfolio-level analysis of SoD effectiveness, drawing on analytics across the full set of control points rather than on point-by-point inspection, is an emerging discipline that supports the identification of systemic weaknesses warranting targeted remediation (Debreceny, 2013; Jans *et al*., 2014).

The literature has also examined the effect of internal audit quality on the identification and remediation of SoD weaknesses. Internal audit functions with high professional qualification, adequate resourcing, and independent reporting lines to the audit committee identify SoD weaknesses earlier and produce more durable remediation than under-resourced or operationally dependent internal audit functions (Gramling *et al*., 2004; Prawitt *et al*., 2009; Sarens, 2009). The investment in internal audit quality is therefore a complement to the investment in access-governance technology, and the two investments should be planned jointly.

A sixth risk dimension, emerging over the review period, concerns third-party and supply-chain access risks. Multinational treasury operations increasingly rely on third-party service providers for payment processing, for confirmation matching, for analytical services, and for cloud-hosted infrastructure. Each third-party relationship creates an additional access surface that must be managed within the organisation's SoD architecture. The specific challenge is that third-party access is typically governed by commercial contracts rather than by internal role structures, and the harmonisation of contract-based and policy-based access controls requires explicit design attention. The emerging discipline of third-party risk management provides useful templates for this harmonisation (Benaroch *et al*., 2012; Debreceny, 2013).

A seventh risk dimension concerns the ethical and conduct-risk implications of SoD weakness. Where SoD is ineffective, individual users who would not otherwise engage in misconduct may be tempted by opportunity, and a small number of users whose conduct intentions are problematic can cause material losses. Conduct-risk mitigation therefore operates alongside fraud-risk mitigation in the design of access governance, and the two dimensions are closely related. Behavioural research on employee misconduct in information-systems environments supplies analytical vocabulary for this discussion, and its integration with the compliance-oriented access-governance literature is an active area of research (Siponen & Vance, 2010; Willison & Warkentin, 2013).

Quantification of the financial consequences of access-governance weakness has been attempted through several approaches. Direct approaches aggregate the losses attributable to identified access-related events (unauthorised payments, fraudulent transactions, settlement failures) across multi-year observation windows. Indirect approaches estimate the costs of compensating controls (manual review, duplicate processing) that are retained because access controls cannot be relied upon. Both approaches produce material cost estimates that support investment in access-governance reform, and both face methodological challenges in attributing costs to specific control weaknesses rather than to broader control-environment features. The academic literature on the cost of weak internal controls provides benchmarks that can inform treasury-specific assessments, though the treasury-specific empirical evidence remains thinner than its practical importance warrants (Benaroch *et al*., 2012; Canada *et al*., 2009).

6. Regulatory Environment and Compliance Interactions

The regulatory landscape for multinational treasury controls comprises several layers. At the group level, SOX Section 404 (for US-listed groups) or equivalent internal-control reporting requirements under local exchanges govern the documentation and testing of internal controls, including treasury controls. Section 404 testing typically reaches into access and SoD controls within the TMS and related systems, and findings at the treasury level can contribute to material weakness determinations at the group level (PCAOB, 2007).

At the entity level, local banking regulations impose specific requirements on payment authorisation, on the handling of customer funds (where applicable), and on the retention of transaction records. Local statutory audits test against local regulatory requirements as well as against group-level control specifications, and the interaction between local and group requirements is a recurring source of design complexity. Access controls that satisfy group-level SoD requirements may not satisfy local requirements, and vice versa, producing compliance tensions that must be resolved at design time rather than at audit time.

At the information-security level, standards such as ISO 27001 and the NIST Cybersecurity Framework (NIST, 2018) specify access-control objectives that apply to treasury platforms as to other information systems. Most multinational groups have adopted one or more of these standards at the information-security policy level, and the specific standards selected shape the access-control practices available to the treasury function. The integration between information-security standards and accounting-control frameworks (COSO, COBIT) is generally managed at the policy level but requires active attention at the operational level to avoid gaps and overlaps.

Data protection regulations, particularly the EU General Data Protection Regulation and national analogues in other jurisdictions, introduce an additional regulatory dimension. Treasury operations process substantial volumes of personal data in the context of supplier and customer payments, and access controls must reflect data-protection principles of purpose limitation, data minimisation, and access restriction to those with a legitimate need. The data-protection dimension is distinct from, but related to, the SoD dimension, and the two dimensions must be jointly addressed in access-governance design (Mbonu *et al*., 2020a).

Emerging regulatory concerns around operational resilience, particularly following the Bank of England and Financial Conduct Authority operational-resilience framework, raise new considerations for treasury access governance. Operational resilience requires that treasury operations continue to function under a range of stress scenarios, including cyber incidents, third-party failures, and physical disruptions. Access-governance design must support operational resilience through mechanisms such as emergency-access procedures, access continuity across sites, and documented recovery procedures that preserve SoD properties under stress conditions (Feng *et al*., 2015; Li *et al*., 2012).

The regulatory interaction with financial-crime compliance adds another layer. Anti-money-laundering, sanctions-screening, and counter-terrorist-financing requirements apply to payments processed by the treasury function, and the access controls that support SoD must also support the segregation required between transaction processing and financial-crime compliance investigation. The segregation is typically operationalised through parallel workflow routing of flagged transactions to financial-crime teams, with compensating controls to ensure that the routing itself cannot be bypassed by users with elevated access. The design of financial-crime-aware access controls is an emerging practice area that intersects with the framework advanced in this article (Fadayomi *et al*., 2021).

The cross-border regulatory dimension is frequently complicated by differences in the scope and stringency of regulatory enforcement across jurisdictions. Treasury policies that are compliant with the letter of each local regulation may nevertheless produce operational inconsistencies that undermine the substantive objective of the regulatory framework. Pragmatic treasury-policy design therefore seeks a globally consistent baseline that is overlaid with jurisdiction-specific supplements, rather than a lowest-

common-denominator or highest-common-denominator approach. The framework's cross-border SoD layer provides the structural basis on which this policy architecture can be operationalised.

The payment-system regulatory environment has evolved materially over the review period, with implications for treasury access governance. The introduction of SEPA in Europe, of real-time payment infrastructures in several emerging-market jurisdictions, and of expanded SWIFT messaging standards has shifted the operational context in which treasury payments are processed. Access-governance design must accommodate the specific features of each payment-system environment, including the authentication requirements, the reconciliation mechanisms, and the dispute-resolution procedures. Real-time payment environments in particular introduce time-compression challenges that stress traditional SoD architectures, because the authorisation step must be completed within the compressed processing window without sacrificing the review quality that SoD is meant to deliver (Chang *et al*., 2014; Hall, 2015).

The interaction between SoD design and the broader information-technology strategy of the organisation warrants explicit attention. Treasury operations increasingly rely on shared identity-management infrastructure (such as Active Directory, enterprise identity-governance platforms, and federated identity arrangements across group entities) rather than on standalone treasury-specific identity stores. The shared infrastructure produces economies of scale and supports consistent identity practice across the organisation, but it introduces dependencies on the security and availability of the shared services. Treasury access-governance architecture must therefore be designed in coordination with the enterprise IT architecture, with specific attention to the access-rights granularity and review cadence that treasury-specific requirements impose on the shared infrastructure (Ferraiolo *et al*., 2001; Rubino & Vitolla, 2014).

Cross-border data-transfer regulations create additional constraints. Where treasury operations process personal data across jurisdictional boundaries, transfer arrangements must comply with local data-protection requirements that may restrict the geographic locations in which data can be stored or processed. The operational implications include the selection of cloud-hosting regions, the design of data-replication arrangements, and the specification of access controls that reflect the residency restrictions imposed by source-jurisdiction regulators. These arrangements must be integrated with the SoD architecture rather than implemented in parallel, because conflicts between data-residency restrictions and SoD requirements have proven difficult to resolve after the fact (Mbonu *et al*., 2020a; Mbonu *et al*., 2020b).

7. Propositions and Research Agenda

Six falsifiable propositions follow from the framework. Proposition 1: multinational treasuries at COBIT Level 3 or above on transactional SoD show unauthorised-payment frequency at least 80 per cent lower than treasuries at Level 1–2, measured over a twelve-month operating window. Proposition 2: functional-SoD maturity (measured by absence of role-conflict exceptions above SOX de minimis thresholds) reduces reconciliation-break volume by at least 40 per cent, controlling for transaction volume. Proposition 3: cross-border SoD maturity (presence of documented shared-service-to-local-treasury boundary controls) reduces severe SOX Section 404 audit findings by at least 60 per cent relative to treasuries without such boundary controls. Proposition 4: the treasury-centralisation-to-effectiveness relationship is inverted-U-shaped, with peak effectiveness at centralisation levels of 60–75 per cent of treasury transactions processed through a regional or global centre, and deterioration above 85 per cent due to local-context blindness. Proposition 5: deployment of identity-governance technology reduces per-user SoD enforcement cost by at least 50 per cent at access-complexity levels above 200 distinct entitlements per user, with smaller effects at lower complexity. Proposition 6: access-governance maturity positively moderates the TMS-capability-to-risk-reduction relationship: the risk-reduction benefit of TMS capability upgrades is at least twice as large in high-access-governance-maturity organisations as in low-maturity organisations. Each proposition specifies the disconfirming condition: absence of the predicted differential at conventional significance thresholds after controlling for firm size, industry, and regulatory context.

The propositions differ in the ease with which they can be tested. Propositions one, two, and three specify relationships between access-governance maturity (measurable through survey or internal audit assessment) and risk outcomes (measurable through incident logs, reconciliation-break registers, and audit findings). These propositions are amenable to cross-firm testing through survey designs with external validation against archival data where available. Proposition four is an interaction claim, requiring measurement of both centralisation and effectiveness across a sample with variation in both; it is testable but requires larger samples. Propositions five and six concern moderating effects that require still larger samples or more sophisticated research designs.

Governance architecture for access management requires attention to three design elements. The first is the access-certification process, through which access rights are periodically reviewed and re-authorised. Certification should be conducted by individuals with sufficient understanding of the roles under review and sufficient authority to challenge excess access. Certification frequency should be calibrated to the risk profile of the access, with higher-risk access certified more frequently (Krishnan & Visvanathan, 2007; Sarens & De Beelde, 2006).

The second is the exception-handling process. Exceptions to SoD rules arise for legitimate reasons, including emergency access, cover for absent staff, and temporary assignments. An effective access-governance architecture provides a structured exception-handling process with explicit approval, documentation, and time-limited duration of the exception. Without such a process, exceptions accumulate into permanent violations of SoD that are difficult to identify and remediate (Spira & Page, 2003).

The third is the monitoring and analytics capability. Modern identity-governance platforms provide analytical tools for the identification of access-right patterns inconsistent with policy, of users with excess or unused access, and of access combinations that violate SoD rules. The analytical capability is the mechanism through which compliance drift is identified and remediated, and its effective use requires investment in the analytics platform and in the staff capability to interpret its outputs (Ge & McVay, 2005; Krishnan & Visvanathan, 2007).

Governance architecture for access management should also include explicit provisions for exception-approval workflows. Business circumstances frequently require deviations from standard SoD rules, and a well-designed governance framework provides structured approval paths for such deviations. The approval workflow should specify the authority required for each class of exception, the documentation that must accompany the approval, the maximum duration of the exception, and the post-exception review that verifies the exception was used only for its intended purpose. Organisations that operate without structured exception workflows typically experience exception proliferation, with deviations granted informally and then persisting indefinitely. The structured approach, by contrast, maintains the integrity of the access architecture while accommodating the operational flexibility that real business conditions require (Bedard & Graham, 2011; Bhaskar *et al*., 2019).

The integration of SoD testing with the external audit process is a further governance dimension. External auditors routinely test access-governance controls as part of their assessment of the control environment supporting financial reporting. The testing scope, timing, and depth affect both the cost of the audit and the reliability of the audit opinion. Effective governance should include structured coordination between internal audit, external audit, and treasury management on the scope of SoD testing, with the objective of maximising the combined assurance value while minimising duplication. Jurisdictions with integrated audit requirements (such as the SOX regime) provide a useful template for this coordination, though the principles apply more broadly across jurisdictions (Bedard, Hoitash, & Hoitash, 2009; Bedard & Graham, 2011).

A final research direction concerns the empirical validation of the three-layer structure itself. The framework advances the three layers as an analytical abstraction; empirical work is needed to determine whether the three layers are distinguishable in practice and whether their interaction operates as the framework proposes. Case-study designs with detailed access to organisational design documentation, supplemented by survey designs that measure perceived SoD effectiveness at each layer, offer suitable research strategies. The validation work would clarify the boundary conditions of the framework and would identify adaptation required for specific organisational contexts (Spira, 2006; Sutton, 2006; Turner & Weickgenannt, 2013; Weber, 1999).

Benefits realisation tracking is an under-emphasised governance dimension. Access-governance reform programmes typically produce both operational benefits (reduced manual controls, faster access provisioning) and risk-reduction benefits (fewer access-related audit findings, lower probability of cyber-enabled fraud). Benefits realisation tracking quantifies these effects over the multi-year horizon of the programme and supports subsequent investment decisions by producing credible evidence of prior-programme effectiveness. Tracking arrangements should be established ahead of programme deployment, with baseline measurements in place before the reform interventions begin, and should continue for at least two years after deployment to capture the stabilisation of reform effects (Canada *et al*., 2009; Weber, 1999).

Six testable propositions linking SoD layer maturity to treasury risk outcomes are summarised in Table 2. The propositions are expressed in a form suitable for empirical testing through comparative case-study or survey-based research designs.

Table 2: Six propositions linking SoD layer maturity to treasury risk outcomes.

#	Independent Variable	Outcome	Predicted Sign
P1	Transactional SoD maturity	Unauthorised-payment frequency	Negative
P2	Functional SoD maturity	Reconciliation-break volume	Negative
P3	Cross-border SoD maturity	Audit-finding severity (Section 404)	Negative
P4	Treasury centralisation	Access-governance effectiveness	Non-linear
P5	Identity-governance technology	SoD enforcement cost	Negative
P6	Access-governance maturity	TMS-outcome relationship strength	Moderating

Three research priorities follow. The first is the effect of emerging identity-governance technologies on the cost of SoD enforcement at scale, which would inform investment decisions by practitioners. The second is the interaction between SOX Section 404 testing and cross-border SoD design, particularly the effect of testing scope on the observed stringency of access governance. The third is the moderating role of treasury centralisation on access-governance effectiveness, which would clarify the non-linearity predicted by the framework. Adjacent work on decision-support analytics for enterprise risk management, capital-allocation decision models based on financial analytics, customer-support quality in digital service environments, and real-time network monitoring across business information systems supplies complementary methodological perspectives that the research agenda can draw on (Lawal & Oduleye, 2021; Morah *et al*., 2021; Nwankwo *et al*., 2021; Ugwu-Oju *et al*., 2021).

A further research direction concerns the application of artificial-intelligence and machine-learning techniques to the detection of SoD policy violations in transaction logs. Rule-based SoD enforcement identifies violations specified in advance, but it cannot identify novel patterns of access abuse that arise from unforeseen combinations of legitimate activities. Pattern-recognition techniques applied to large-scale transaction-log datasets offer the prospect of identifying novel violation patterns at scale, and their integration with rule-based enforcement represents a frontier of access-governance research (Debreceny, 2013; Grabski *et al*., 2011; Jans *et al*., 2014).

A final research direction concerns the empirical validation of the three-layer structure itself. The framework advances the three layers as an analytical abstraction; empirical work is needed to determine whether the three layers are distinguishable in practice and whether their interaction operates as the framework proposes. Case-study designs with

detailed access to organisational design documentation, supplemented by survey designs that measure perceived SoD effectiveness at each layer, offer suitable research strategies. The validation work would clarify the boundary conditions of the framework and would identify adaptation required for specific organisational contexts (Spira, 2006; Sutton, 2006; Turner & Weickgenannt, 2013; Weber, 1999).

8. Conclusion

This article has developed a cross-border SoD and access-governance framework for multinational treasury. The framework distinguishes three control layers: transactional SoD within the TMS, functional SoD across treasury teams, and cross-border SoD between shared-service centres and local treasuries. Six propositions link access-governance maturity to treasury-specific risk outcomes, each amenable to empirical testing through survey, archival, or mixed-method research designs.

The central analytical contribution is the explicit treatment of cross-border SoD as a distinct control layer with distinctive design challenges. Existing literature treats SoD primarily as a transactional or functional problem, and under-examines the cross-border dimension that has become increasingly material as multinational treasury structures have matured. By providing a structured vocabulary for the cross-border layer, the framework supports both practitioner design work and academic investigation of a dimension that has been under-examined relative to its practical importance.

For practitioners, the framework offers a diagnostic instrument for treasury access-governance assessment and an organising vocabulary for access-governance reform programmes. For researchers, it offers testable propositions and a structured vocabulary that supports cumulative empirical work. The cumulative contribution is intended to raise the analytical precision of both practitioner diagnosis and academic investigation of an increasingly important dimension of treasury control in multinational organisations. The framework's value will ultimately be measured by its uptake in both communities and by the quality of the empirical and practical work it supports over subsequent years.

The framework also complements the emerging body of conceptual work on segregation of duties as a design problem rather than a procedural requirement. Kobelsky (2014) argues that conventional SoD rule sets, developed for single-jurisdiction operations, systematically under-specify the organisational design choices that actually determine control effectiveness, and proposes a design-theoretic alternative grounded in explicit organisational archetypes. The three-layer framework developed here is consistent with this design-theoretic orientation and extends it by identifying the specific cross-border features of multinational treasury that require explicit architectural treatment. Subsequent empirical work calibrating the three layers against observed practice in specific multinational groups will provide the validation base from which further refinement of the framework can proceed.

The broader implications for the multinational treasury function extend beyond the access-governance topic treated here. The three-layer analytical structure generalises to other dimensions of multinational treasury design, including the allocation of hedging responsibility between central and local teams, the integration of liquidity management across entities, the management of counterparty-credit risk across subsidiary banking relationships, and the coordination of regulatory-compliance activities across jurisdictions. Each of these dimensions presents similar tensions between the efficiency advantages of centralisation and the control advantages of local responsiveness, and each can be examined through the three-layer lens developed in this article. Subsequent research extending the framework to these adjacent dimensions would produce an integrated analytical vocabulary for multinational treasury design that is currently lacking in the literature.

The article also speaks to broader discussions about the governance of distributed operational activity in multinational organisations. Treasury is one of several functions in which operational activity is distributed across jurisdictions with shared technology platforms and with varying degrees of centralisation; others include tax, internal audit, procurement, and human resources. The analytical challenges examined here, particularly the reconciliation of global efficiency with local responsiveness and the management of compliance drift over multi-year operation, apply with modifications to each of these functions. The framework advanced here may therefore be of use to researchers and practitioners working on these adjacent topics, with adaptations that reflect the specific operational features of each function.

Policy and regulatory implications of the framework are also worth brief consideration. Regulators responsible for the oversight of financial reporting controls can use the framework as a basis for examining the adequacy of access governance at regulated entities, with particular attention to the cross-border dimension that existing examination protocols tend to under-emphasise. Standard-setting bodies responsible for auditing standards can use the framework to structure guidance on the testing of access controls in multinational-group audits. Professional bodies responsible for treasury certification can use the framework to structure the access-governance content of certification curricula. Each of these applications would reinforce the cumulative contribution of the framework to the governance of access in multinational financial operations.

References

1. Ashbaugh-Skaife H, Collins DW, Kinney WR, LaFond R. The effect of SOX internal control deficiencies and their remediation on accrual quality. Accounting Review. 2008;83(1):217–250.
2. Bertino E, Ferrari E. Big data security and privacy. In: Flesca S, Greco S, Masciari E, Sacca D, editors. A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years. Springer; 2018. p. 425–439.
3. Bhaskar LS, Schroeder JH, Shepardson ML. Integration of internal control and financial statement audits: Are two audits better than one? Accounting Review. 2019;94(2):53–81.
4. Chalmers K, Hay D, Khlif H. Internal control in accounting research: A review. Journal of Accounting Literature. 2019;42:80–103.
5. COSO. Internal Control–Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission; 2013.
6. Doyle JT, Ge W, McVay S. Determinants of weaknesses in internal control over financial reporting. Journal of Accounting and Economics. 2007;44(1–2):193–223.
7. Fadayomi O, Bello AD, Elebe O, Hammed NI, Omoegun

GO. An integrated cybersecurity and anti-money laundering framework for enterprise financial systems. IRE Journals. 2021.
8. Feng M, Li C, McVay S, Skaife H. Does ineffective internal control over financial reporting affect a firm's operations? Evidence from firms' inventory management. Accounting Review. 2015;90(2):529–557.
9. Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chandramouli R. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security. 2001;4(3):224–274.
10. Ge W, McVay S. The disclosure of material weaknesses in internal control after the Sarbanes-Oxley Act. Accounting Horizons. 2005;19(3):137–158.
11. Gregor S, Jones D. The anatomy of a design theory. Journal of the Association for Information Systems. 2007;8(5):312–335.
12. Hoitash R, Hoitash U, Bedard JC. Corporate governance and internal control over financial reporting: A comparison of regulatory regimes. Accounting Review. 2009;84(3):839–867.
13. Institute of Internal Auditors (IIA). The IIA's Three Lines Model: An Update of the Three Lines of Defense. IIA; 2020.
14. ISACA. COBIT 2019 Framework: Governance and Management Objectives. ISACA; 2019.
15. Jensen MC, Meckling WH. Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics. 1976;3(4):305–360.
16. Kinney WR. Research opportunities in internal control quality and quality assurance. Auditing: A Journal of Practice and Theory. 2000;19(s-1):83–90.
17. Klamm BK, Watson MW. SOX 404 reported internal control weaknesses: A test of COSO framework components and information technology. Journal of Information Systems. 2009;23(2):1–23.
18. Krishnan J, Visvanathan G. Reporting internal control deficiencies in the post-Sarbanes-Oxley era: The role of auditors and corporate governance. International Journal of Auditing. 2007;11(2):73–90.
19. Lawal OA, Oduleye TE. A conceptual decision model for capital allocation using financial analytics. Gyanshauryam, International Scientific Refereed Research Journal. 2021;4(2):269–295.
20. Li C, Peters GF, Richardson VJ, Weidenmier Watson M. The consequences of information technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports. MIS Quarterly. 2012;36(1):179–203.
21. Mbonu IS, Aliliele C, Iwuanyanwu U, Uzoka E. A review of identity and access management integration strategies in hybrid and multi cloud environments. International Journal of Multidisciplinary Research and Growth Evaluation. 2020;1(5):795–810.
22. Mbonu IS, Iwuanyanwu U, Aliliele C, Uzoka E. Advances in infrastructure as code governance for secure Terraform based enterprise cloud deployments. International Journal of Multidisciplinary Research and Growth Evaluation. 2020;1(5):811–828.
23. Morah OO, Ekpedo L, Awanye EN, Adeyoyin O, Agbosu EK. Advances in decision support analytics improving enterprise risk management effectiveness outcomes measures. Gyanshauryam, International Scientific Refereed Research Journal. 2021;4(2):296–317.
24. Nandi S, Kumar A. Centralisation and the success of ERP implementation. Journal of Enterprise Information Management. 2016;29(5):728–750.
25. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. NIST; 2018.
26. Nwankwo CO, Okeke OT, Ugwu-Oju UM. Conceptual model improving customer support quality within digital service environments. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2021;7(2):721–734.
27. Oshoba TO, Hammed NI, Odejobi OD. A systems framework for secure enterprise deployment of software and infrastructure components. Iconic Research and Engineering Journals. 2019;3(2):428–446.
28. Oshoba TO, Hammed NI, Odejobi OD, Michael C. Advances in strong multi-factor authentication and user identity enforcement in enterprise payment and messaging platforms. Iconic Research and Engineering Journals. 2021;5(4):408–427.
29. PCAOB. Auditing Standard No. 5: An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements. Public Company Accounting Oversight Board; 2007.
30. Polak P. The centre holds: From the decentralised treasury towards fully centralised cash and treasury management. Journal of Corporate Treasury Management. 2009;3(2):109–112.
31. Polak P, Kocurek K. Cash and working capital management in the Czech Republic. Investment Management and Financial Innovations. 2007;4(1):17–24.
32. Power M. The Audit Society: Rituals of Verification. Oxford University Press; 1997.
33. Sarens G, De Beelde I. Internal auditors' perception about their role in risk management: A comparison between US and Belgian companies. Managerial Auditing Journal. 2006;21(1):63–80.
34. Siponen M, Vance A. Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly. 2010;34(3):487–502.
35. Spira LF, Page M. Risk management: The reinvention of internal control and the changing role of internal audit. Accounting, Auditing and Accountability Journal. 2003;16(4):640–661.
36. Turner L. Use ERP internal control exception reports to monitor and improve controls. Management Accounting Quarterly. 2006;8(1):8–23.
37. Ugwu-Oju UM, Nwankwo CO, Okeke OT. Conceptual model improving real-time network monitoring across business information systems. International Journal of Scientific Research in Science and Technology. 2021;8(5):715–732.
38. Warkentin M, Willison R. Behavioral and policy issues in information systems security: The insider threat. European Journal of Information Systems. 2009;18(2):101–105.
39. Wright C. Fraud Prevention and Internal Audit. ICSA Publishing; 2008.
40. Quattrone P, Hopper T. A "time-space odyssey": Management control systems in two multinational organisations. Accounting, Organizations and Society.

2005;30(7–8):735–764.
41. Bedard JC, Graham L. Detection and severity classifications of Sarbanes-Oxley Section 404 internal control deficiencies. Accounting Review. 2011;86(3):825–855.
42. Bedard JC, Hoitash R, Hoitash U. Evidence from the United States on the effect of auditor involvement in assessing internal control over financial reporting. International Journal of Auditing. 2009;13(2):105–125.
43. Benaroch M, Chernobai A, Goldstein J. An internal control perspective on the market value consequences of IT operational risk events. International Journal of Accounting Information Systems. 2012;13(4):357–381.
44. Canada J, Sutton SG, Kuhn JR. The pervasive nature of IT controls: An examination of material weaknesses in IT controls and audit fees. International Journal of Accounting and Information Management. 2009;17(1):106–119.
45. Cerullo V, Cerullo MJ. Threat assessment and security measures justification for advanced IT networks. Information Systems Control Journal. 2005;1:43–46.
46. Chang SI, Yen DC, Chang IC, Jan D. Internal control framework for a compliant ERP system. Information & Management. 2014;51(2):187–205.
47. Colbert JL, Bowen PL. A comparison of internal controls: COBIT, SAC, COSO and SAS 55/78. IS Audit and Control Journal. 1996;4:26–35.
48. Debreceny RS. Research on IT governance, risk, and value: Challenges and opportunities. Journal of Information Systems. 2013;27(1):129–135.
49. Grabski SV, Leech SA, Schmidt PJ. A review of ERP research: A future agenda for accounting information systems. Journal of Information Systems. 2011;25(1):37–78.
50. Gramling AA, Maletta MJ, Schneider A, Church BK. The role of the internal audit function in corporate governance. Journal of Accounting Literature. 2004;23:194–244.
51. Hall JA. Information Technology Auditing. 4th ed. Cengage Learning; 2015.
52. Jans M, Alles MG, Vasarhelyi MA. A field study on the use of process mining of event logs as an analytical procedure in auditing. Accounting Review. 2014;89(5):1751–1773.
53. Kuhn JR, Sutton SG. Continuous auditing in ERP system environments: The current state and future directions. Journal of Information Systems. 2010;24(1):91–112.
54. Messier WF, Glover SM, Prawitt DF. Auditing and Assurance Services: A Systematic Approach. 10th ed. McGraw-Hill; 2017.
55. Morris JJ. The impact of enterprise resource planning (ERP) systems on the effectiveness of internal controls over financial reporting. Journal of Information Systems. 2011;25(1):129–157.
56. O'Leary DE. Enterprise Resource Planning Systems: Systems, Life Cycle, Electronic Commerce, and Risk. Cambridge University Press; 2000.
57. Prawitt DF, Smith JL, Wood DA. Internal audit quality and earnings management. Accounting Review. 2009;84(4):1255–1280.
58. Rubino M, Vitolla F. Corporate governance and the information system: How a framework for IT governance supports ERM. Corporate Governance. 2014;14(3):320–338.
59. Sarens G. Internal auditing research: Where are we going? International Journal of Auditing. 2009;13(1):1–7.
60. Spira LF. Black boxes, red herrings and white powder: UK audit committees in the 21st century. Journal of Banking Regulation. 2006;7(1–2):180–188.
61. Sutton SG. Enterprise systems and the re-shaping of accounting systems: A call for research. International Journal of Accounting Information Systems. 2006;7(1):1–6.
62. Turner L, Weickgenannt A. Accounting Information Systems: Controls and Processes. 2nd ed. Wiley; 2013.
63. Weber R. Information Systems Control and Audit. Prentice Hall; 1999.
64. Willison R, Warkentin M. Beyond deterrence: An expanded view of employee computer abuse. MIS Quarterly. 2013;37(1):1–20.
65. Kobelsky KW. A conceptual model for segregation of duties: Integrating theory and practice. International Journal of Accounting Information Systems. 2014;15(4):304–322.