International Journal of Humanities and Information Technology (IJHIT)
e-ISSN: 2456 –1142, Volume 6, Issue 4, (December 2024), www.ijhit.info

Role-Based Access and Segregation-of-Duties Monitoring in ERP Financial Systems with Behavioral Anomaly Scoring

Ifeoma E. Okoli[1], Deborah Ujeh Osahor[2*], Carol Kpobie[3], Friday Odihi[4]

[1]*Maersk Logistics, Canada;* Ifeomaokoli47@gmail.com

[2]*Georgia Southern University, United States;* osahordeborah@gmail.com

[3]*Deloitte & Touche LLP, Accra, Ghana;* msckpobie@gmail.com

[4]*Joseph Sarwuan Tarka University (formerly Federal University of Agriculture, Makurdi), Nigeria;* odihison@gmail.com

***Corresponding author:** Deborah Ujeh Osahor, osahordeborah@gmail.com

Abstract

Separation of duties is one of the earliest technical controls in financial systems, and the standard monitoring approach in enterprise resource planning (ERP) is based on comparing role assignments against a static list of permission pairs, which are known as segregation-of-duties conflicts. This approach is auditable and cheap, but it cannot capture the conflicts emerging from combinations of individually compatible permissions, from fragmented rules, or from sequential user actions. This paper defines a monitoring architecture, which maintains a static conflict matrix as the decision-making authority, and adds two more layers, behavioral and sequence layers, which compare each user-transaction pair to the historical behavior of the user and her structurally similar peers, and to the reconstructed sequences of users, respectively. The paper formally defines effective permission computation, conflict specifications based on scope predicates, and the remediation decision problem in the presence of a limited reviewer capacity. It defines latent conflicts in one place and uses the definition in the rest of the paper. The paper also defines the protocol of evaluating behavioral layer performance, in which each comparison arm is compared against labeled populations of adverse cases at fixed reviewer capacities. The paper does not describe any empirical outcome. Its contribution is the architecture itself, the formal foundation behind it, the governance conditions under which behavioral scores can be employed, and the protocol, whose results need to be measured before the economics of the architecture can be assessed.

Keywords: Segregation of duties; role-based access control; ERP; SAP; Oracle; internal control; behavioral anomaly detection; SoD conflict monitoring; access governance

DOI: 10.21590/ijhit.06.04.49

1. Introduction

Segregation of duties is one of the earliest controls in financial systems, and one of the most persistently violated ones. In ERP systems, the control relies on proper assignment of roles and permissions, and changes to those assignments are supposed to be managed properly. In the ERP

world, monitoring is the way to do that. The paper examines how such monitoring can be designed. It presents an architecture for monitoring segregation of duties, formalizes its decision problems, defines behavioral aspects of the architecture, and states the governance conditions under which the outputs of the architecture can be employed. It does not provide any empirical outcomes. When it suggests an evaluation, it describes the protocol and leaves measurement of results to another reproducible study (Brickley, 2021; Kobelsky, 2014).

1.1 The control and its erosion

Segregation of duties is based on the simple idea that the person, who can both initiate a transaction and cover up her tracks, can commit fraud undetected. This control prevents it by dividing transactions into steps, assigned to different people (Brickley, 2021; Kobelsky, 2014). This is what ERP platforms achieve via authorization objects, profiles and role assignments, which can be altered without modifying any program (Ogbole, 2021; Ratliff, 2022). Since these assignments are frequently updated, permissions accumulate and segregation decays over time rather than fails abruptly (Unamma, 2024; Navandar, 2024). This is why segregation of duties requires monitoring, not just design. The decay is also evident from the audits of continuous monitoring of controls (Kuhn, 2010).

1.2 What static conflict monitoring does and does not do

A common solution to this problem is the segregation of duties conflict matrix, a list of permission pairs, which should not be co-assigned to one user. All major ERP platforms have such matrices, and they are among the standard objects of ERP control testing (Proctor, 2007; Khan, 2010). There are three fundamental limitations to this structure. Its completeness is assumed, not proven, because the conflicts, which depend on the process, entity or jurisdiction, are usually added to it too late, if at all. It operates on one user at a time, and therefore cannot find the violations, which require several users, each possessing an innocent set of permissions. If it is applied to role names or transaction codes, it generates lots of false positives and misses the conflicts, which involve sets of permissions assigned differently in different roles (Sandhu, 1996; Vaidya, 2007).

1.3 The behavioral proposition

The behavioral layer overcomes the second and the third limits but does not replace the matrix itself. The layer has two parts. The first one is a self-model that describes the established user's pattern of behavior over a trailing window. The other is a peer model, and that is users that are structurally comparable based on the role, organizational unit and function assignment. The deviation of a particular user-transaction combination from both models is used for the anomaly scoring (Chandola, 2009; Ominyi, 2024a). Anomaly scoring of this type is a prioritization signal. The register is ordered based on the evidence of the exercised authority, the inconsistency of the behavior with the assigned role, and finally, thanks to the sequence layer discussed in Section 6,

the activity that affects several users is found (Fadayomi, 2024; Okwesa, 2024). The two models address different questions, and thus, each score is justified on its own merits.

2. ERP Authorization Model and the Segregation-of-Duties Construct

This section defines the technical environment where the architecture works. The ERP authorization model defines what can be done by the user at the moment of performing an action, and the segregation of duties construct defines what combinations of capabilities are prohibited. The distinction is the key to choosing the appropriate test. The rule about the capability is evaluated against the effective permissions, which can be calculated from the configuration, while the rule about the activity is evaluated against the event log, which records the performed action. Both are used in the architecture, and the formal treatment in Section 4 relies on the strict separation between the two (Dosunmu, 2019; Kobelsky, 2014). Each of these results is formalized in Section 4, and the tiered architecture of Section 6 is built on the basis of these results.

2.1 Authorization objects and the permission graph

In the standard ERP authorization model, the user can perform the action if the check against the authorization object returns success at the moment of attempting (Khan, 2009; Sandhu, 1996). Thus, the authority of the user is field-valued and not transactional. Users with the same transaction code may have different authorities if the authorization fields differ, e.g., in company code, plant, or account group. The matrix that evaluates the transaction codes alone over-reports due to that reason, and the matrix that evaluates role names alone fails to identify authority that consists of several roles (Vaidya, 2007). The permission graph is bipartite, connecting the users and authorization instances, where the roles are bundles of instances and composite roles are nested in the latter. The effective authority is the closure of the graph at the moment of the check.

2.2 The segregation-of-duties construct

The matrix operationalizes the rule of the type "no user shall be able to perform both A and B", such as creation of the vendor and paying him (Kobelsky, 2014; Proctor, 2007). These rules address the capability and not the activity. The prohibition addresses the ability of performing these actions, and thus the static test of the effective permissions is the appropriate test for the rule as it is written, while the behavioral test identifies the exercise of the capability and answers a different question. The conflicts are not transitive: If A conflicts with B, and B conflicts with C, then A does not necessarily conflict with C. The role with A and a role equivalent to B constitutes a real conflict that the rule in role names will fail to detect (Vaidya, 2007; Brickley, 2021).

2.3 The remediation and mitigation decision

Once the conflict is identified, the decision problem of Section 4.4 selects from four actions. The organization can remediate the issue by removing a conflicting permission, which might lead to

loss of necessary ability. It can redesign the role, separating the permissions, but preserving the process, which is the most durable solution and often also the most expensive. It can mitigate by implementing a compensating control, or accept the risk of the conflict, formally or de facto by leaving the finding in the register (Aneke, 2023; Stamatović, 2020). The four options have different costs and residual risks, which are explicitly accounted in Section 4.4. The behavioral evidence helps to choose the option by demonstrating the match between the exercised authority and the assigned authority.

3. Literature

The architecture is situated relative to research on role-based access control and its ERP instantiations, and in audit research on segregation of duties and continuous auditing. This review is selective. Its goal is to outline the work that backs up the architecture, and also where it diverges from that work. The two fields are read in tandem, because the architecture matrix derives its terminology from access control and its test design from audit practice. Process anomaly detection and process mining techniques are discussed where the behavioral and sequence layers are defined in Sections 5 and 6 (Chandola, 2009). Section 3.1 discusses the audit literature and reviews the ERP tooling in it (Sandhu, 1996; Khan, 2010).

3.1 The audit literature on segregation of duties

In role-based access control permissions are assigned to roles, and roles are assigned to users. Segregation of duties was among the constraints in the original formulation, which required no user hold two specified roles simultaneously (Sandhu, 1996). Audit literature treats segregation of duties as a control activity. Segregation theory and practice are integrated for manual and IT process through a conceptual model (Kobelsky, 2014). Later work analyzes deployment and assessment of least-privilege and segregation policies (Brickley, 2021). Early ERP-specific treatments categorized segregation-of-duties controls as a distinct class of tooling (Proctor, 2007). Continuous auditing in ERP systems takes the issue of timing into account, since a control that is tested once per year does not detect drift between tests (Kuhn, 2010; Gonçalves, 2022).

4. Formalization

This section sets out the formal foundation of the architecture. Notation is introduced once, and used through-out. This is where effective permissions, conflict specifications, the static conflict relation, and the latent-conflict construct on which the evaluation is based are defined. The formalism is grounded in the role-based model, in which permissions are grouped in roles, and roles are assigned to users (Sandhu, 1996; Vaidya, 2007), with scope predicates and time validity added to the basic model. Every definition is stated at the level necessary for the evaluation, so that a reader can derive a flag independently from the stated inputs, without regard to any particular implementation.

4.1 Entities and relations

Let U be the set of users, P the set of permissions and R the set of roles. A permission is an authorization instance. A role is a pair $(P_r, \preceq_r)$ in which $P_r \subseteq P$ and $\preceq_r$ is a partial order that encodes composite structure. The assignment relation $A_t \subseteq U \times R$ records which roles each user holds at time t, so that validity is a property of the assignment rather than of the role. The effective permission set of a user u at time t is

$$\text{Eff}(u,t) = \{\, p \in P : \exists\, r \in R, (u,r) \in A_t \text{ and } p \in \text{expand}(r) \,\} \quad (1)$$

where expand resolves a role to its transitive permission closure, including composite roles and inherited authorizations, evaluated against the field values and validity dates of the assignment. Computing Eff correctly is the technical prerequisite for every later analysis (Sandhu, 1996; Khan, 2009).

4.2 Conflict specification

A conflict specification is a finite set $C = \{c_1, \ldots, c_m\}$ of triples $c_i = (P_i^a, P_i^b, \sigma_i)$. Each side is a permission set that must not be co-held, and the scope predicate σ_i restricts the conflict to a context such as a company code, a process or a materiality threshold. A user is in static conflict with respect to c_i at time t when $\text{Eff}(u,t) \cap P_i^a \neq \emptyset$, $\text{Eff}(u,t) \cap P_i^b \neq \emptyset$ and $\sigma_i(u,t) = 1$. Stating each side as a permission set rather than a role name lets the test see authority spread across roles, and each side and predicate is therefore testable against a user's effective permission set (Sandhu, 1996; Vaidya, 2007). The predicate is evaluated for the same user and time as the permission sets it qualifies.

4.3 Latent conflicts

A transaction cycle is a sequence of steps $s_1, \ldots, s_k$, each requiring a permission. The cycle is segregated if no single user holds two adjacent steps and no pair of users can execute it without an independent check. This paper uses one definition of a latent conflict throughout. A latent conflict is a non-segregated transaction cycle in which no rule in C identifies the combination of permissions, scopes or users that realizes the violation. The definition is relative to the specification and not to the detection method. A latent conflict is therefore not a permanent property of a user, and a conflict that is latent under one specification may be named under a richer one.

Latent conflicts appear in three ways, summarized in Table 1. Set equivalence: the rule refers to one permission when the process requires a set of functionally equivalent permissions. Scope fragmentation: the user holds the two permissions in different company codes, and no rule predicate covers both. Cross-user sequence: Two users hold adjacent steps, and no rule refers to either user (Kobelsky, 2014; Debreceny, 2010).

Table 1. Ways in which latent conflicts arise and the detection they require.

Mechanism	Why no rule names the violation	Detection requirement
Set equivalence	The rule names one permission where the process requires a set of functionally equivalent permissions	Sufficient-set form of the specification (Section 8.1)
Scope fragmentation	The rule's scope predicate is confined to one company code, so a combination across codes lies outside every predicate	Scope predicate that covers the cross-code combination
Cross-user sequence	The rule tests one user at a time, and the violation requires two or more users	Sequence reconstruction across users (tier 3, Section 6.1)

4.4 The decision problem

The organization must choose, for each detected conflict j, an action a_j from the set {remediate, redesign, mitigate, accept}. Let c_{aj} be the cost of action a for conflict j, let ρ_{aj} be the residual risk after action a, and let L_j be the expected loss from conflict j if it is exploited. The decision problem chooses actions to minimize the total cost of control plus expected loss, subject to capacity:

$$\min_{\{a_j\}} \sum_j \left(c_{a_j j} + \rho_{a_j j} L_j \right) \quad \text{subject to} \quad \sum_j 1[a_j \in \{\text{remediate}, \text{redesign}\}] \leq K \qquad (2)$$

where K is the remediation capacity per period. The objective makes explicit that behavioral evidence can change the ordering and the loss estimates L_j, but not the feasible set of actions. The residual risks and losses come from outside the detection system, and the ordering that results is only as reliable as those estimates (Eboh, 2024; Aneke, 2023).

5. Behavioral Feature Family

The behavioral layer defines a family of features for each user and period in five classes based on the type of evidence they carry. Authority-exercise features capture the extent of the use of the authority. Separation-bypass features capture activities which defeat separation in a process. Temporal and volume features capture departures from the rhythm of the user. Relational features locate the user in the approval and master data network. Suppressors lower the score because they capture a valid explanation. Sections 5.1 to 5.6 define the design principle and each of the classes, while each feature is specified relative to one of the three comparison groups (Ominyi, 2024a; Okwesa, 2024). Every feature is specified below with its comparison group such that the score may be audited feature by feature.

5.1 Design principle

Three comparison groups are used. The self group consists of the history of the user in a trailing window. The peer group is made up of users with similar permissions in similar organizational units. The process group gives volume and timing baseline for each transaction type. Each feature is marked with the group against which it is computed. Self relative features detect deviation in the behavior of a user, peer relative features detect behavior which is abnormal for the role of the user, and process relative features detect unusual behavior for the process regardless of who does it. The three groups ask different questions, and hence a combined score of the three without labelling obscures which question the score addresses (Gama, 2014; Fadayomi, 2024).

5.2 Authority-exercise features

Authority exercise features compare the authority that the user holds with the authority that he exercises. The features connect the static and behavioral layers because an assigned but unexercised conflict carries a different risk from an exercised conflict (Khan, 2009; Brickley, 2021).

f_1, fraction of held permissions exercised in the trailing period (self group).

f_2, exercise count and value for each permission in a conflicting pair, computed per side (self group) (Braun, 2003).

f_3, recency of first exercise of each conflicting permission relative to assignment (self group) (Alles, 2002).

f_4, exercise outside the user's peer pattern, weighted by the size of the excess (peer group) (Ashcroft, 2002).

f_5, effective permission count relative to the peer median, and the ratio of directly assigned to role-derived permissions (peer group) (Bolton, 2002).

5.3 Separation-bypass features

Separation-bypass features measure activity that defeats separation directly, rather than the authority that makes it possible. Feature f_6 operates on single transactions. Features f_7 to f_{10} are process-group features that operate on approval paths and on process instances reconstructed from the event log, and they constitute the tier-3 features of Section 6.1 (Okwesa, 2024; Jans, 2014).

f_6, transactions posted by the user and subsequently reversed or adjusted by the same user within a short window (self group) (Rezaee, 2002).

f_7, transactions the user approved where the originator is the same person, or shares a manager with no intervening approval (process group) (Bierstaker, 2001; Ominyi, 2024a).

f_8, sequence entropy, the diversity of step orderings in which the user participates, relative to the modal ordering (process group) (Jans, 2013).

f_9, whether the user both initiates and completes a process instance with no intervening actor (process group) (Semi, 2024; Jans, 2014).

f_{10}, count of process instances in which the user's action was the sole approval above a materiality threshold (process group) (Jans, 2014).

5.4 Temporal and volume features

Temporal and volume features detect departures from the rhythm of the user. They are weak individually because volume and timing are bound to deviate for legitimate reasons, but they are cheap to compute and help distinguish a behavioral deviation from a change in role. They are kept as inputs to the score (Einkamerer, 2017; Gama, 2014).

f_{11}, transaction volume relative to the user's own trailing distribution, as a robust z-score (self group).

f_{12}, activity outside the user's established working hours, estimated from the user's own history (self group).

f_{13}, period-end concentration, the share of monthly activity in the final three business days relative to the user's baseline (self group).

f_{14}, change in the composition of the user's activity, measured by Jensen-Shannon divergence against the trailing baseline (self group) (Gama, 2014).

5.5 Relational features

Relational features locate the user in the approval and master data network. The value of the features lies in their relationship with other actors, making them sensitive to network structure and thus needing the peer normalization of Section 5.1 (Akoglu, 2015; Vasarhelyi, 2015).

f_{15}, distinct users sharing an approval path with this user in the trailing period, normalized by the peer median (peer group) (Unamma, 2024).

f_{16}, concentration of the user's transactions on a small set of master-data records, such as one vendor or bank account (process group) (Alles, 2016).

f_{17}, whether the user created or modified master data for an entity that later appears in transactions the user approved (process group) (Vasarhelyi, 2015).

f_{18}, degree-normalized betweenness of the user in the approval network (peer group) (Akoglu, 2015).

f_{19}, overlap of the user's approval network with an unusual vendor segment (process group) (Adelanwa, 2023b).

5.6 Suppressors and the legitimate-explanation problem

This leads to false positives characterized mainly by innocent reasons such as change of role, delegation record and a small organizational unit. There are four suppressors that decrease the score of such a reason. They are neither proof of innocence nor they can clear a conflict. All that they do is they alter the order of flags and the evidence of the same (Adeniji, 2023; Adesuyi, 2023).

s_1, days since the most recent role or permission change, with a decay function, so that a recent change lowers the score for a limited period (Unamma, 2024).

s_2, documented delegation or coverage arrangement for the period, drawn from an HR or workflow system where available.

s_3, organizational unit with fewer than the minimum peer group size, in which case peer-relative features are shrunk toward the global distribution.

s_4, anomalous activity bounded to a project code or cost center with a documented exceptional authorization (Adesuyi, 2023).

6. Architecture

There are three levels in the architecture. These levels have different functions and evidential status and the differentiation between them is the key governance attribute of the design. The first level is deterministic and defines the permissions of the user. The second level ranks the flags and provides their description based on observed behavior. The third level recreates activity of users. These levels are organized in such way that the evidence based on behavioral information does not lead to changes in the register on its own and every finding on a sequence has another evidential path prior to any action (Sandhu, 1996; Adeyelu, 2023). Anyone interested in auditing a flag will be able to trace it from the level of its appearance through evidence and to the source rule or feature generating the flag.

6.1 Three tiers

Tier 1, effective permission analysis, computes Eff(u, t) for every user in each period, resolves composite roles and direct assignments, evaluates the conflict specification with its scope predicates, and produces the conflict register, deterministically and reproducibly from a configuration snapshot. Tier 2, behavioral scoring, computes the Section 5 features for each user and period, produces a score, and attaches component evidence to each conflict. It ranks and informs but does not add or remove conflicts. Tier 3, sequence analysis, reconstructs process instances from the event log, computes features f_7 to f_{10}, and flags instances in which

separation was not effective. Its findings require separate governance and a documented evidential pathway before action (Adeyelu, 2023; van der Aalst, 2016).

6.2 Score composition and attribution

Each feature is standardized within its comparison group, and shrunk toward the global distribution where the group is small. Standardization keeps features with different units comparable within the score. Write g_j for the standardized form of f_j. The user score is a weighted combination of the standardized risk features less a weighted sum of the suppressors:

$$z_{u,t} = \sum_j \beta_j g_j(u,t) - \sum_k \gamma_k s_k(u,t), \quad \beta_j \geq 0, \quad \gamma_k \geq 0 \tag{3}$$

Weights being non-negative lead to monotonicity of the score relative to exercised authority: increasing the exercised authority in a conflicting pair increases the score. Since the score is additive, every contribution can be reported along with the corresponding conflict, thus providing the evidence that tier 2 needs to attach to every flag (Lundberg, 2017; Ribeiro, 2016).

7. Evaluation Protocol

The evaluation protocol is a design for reproducible research. The paper does not report any results but the protocol prescribes a fixed population design, comparison arms, metrics, the adverse classes and capacity constraints that are specified beforehand and therefore enable reading the results of a future study against a predetermined specification rather than a configuration chosen on-the-fly. Every element can be carried out on a synthetic population with ground-truth labels or on an installation with audited outcomes and the reporting requirements of Section 7.7 apply to both cases (Gama, 2014; Hemati, 2021). The arms and the quantities are defined in the next sections in order to enable future studies against this specification.

7.1 Population specification

The population for evaluation is generated or sampled with the following parameters fixed beforehand regardless of which arm is run: the numbers of users, organizational units and company codes; the numbers of roles and distinct permission instances; the number of months; the numbers of conflict rules and the fraction of the rules having a scope predicate; and the fraction of the users having assignments inconsistent with the role template of their unit. This latter parameter controls the latent exposure in the population and it is chosen from the design not based on any observation (Khan, 2009; Vaidya, 2007).

The conflict specification itself is intentionally incomplete. The population has conflicts that have no rules specified, such that the protocol tests not only the static but also the latent detection capacity. The generative process itself, the seed and the values of the parameters for each population are published along with the research, making it possible to regenerate the population (Khan, 2009; Brickley, 2021).

7.2 Comparison arms

The five comparison arms are shown in Table 2. Arm A1 represents a traditional implementation of the static approach using role names without resolving the permission effectiveness. Arm A2 consists of effective permission analysis using the set-based rules with the scope predicate and temporal validity but no behavioral component. Arm A3 represents the behavioral scoring technique with prior weights but no conflict specification. Arm A4 is an amalgamation of A2 as the authority exercise and A3 as prioritization using the expected loss metric, while A5 adds the tier-3 features to A4. Comparing A1 to A2 isolates the extraction layer, while comparing A4 to A2 isolates the behavioral evidence contribution (Proctor, 2007; Kobelsky, 2014). Table 2 shows the components of each arm.

Table 2. Comparison arms, detection authority and prioritization components.

Arm	Detection authority	Prioritization or evidence	Sequence features
A1	Role-name conflict test	None	No
A2	Effective permission analysis with scope predicates	None	No
A3	None (no conflict specification)	Behavioral features of Section 5 with prior weights	No
A4	A2	A3, ranked by expected loss	No
A5	A2	A3, ranked by expected loss	Yes (f7 to f10)

7.3 Metrics and capacity constraint

The primary metric is precision at a reviewer capacity of 0.5 per cent of users flagged per period. Let $F_t(\kappa)$ be the set of users flagged in period t at capacity κ, so that $|F_t(\kappa)| \leq \kappa |U|$, and let A be the set of adverse users. Precision at capacity is

$$P@\kappa = \frac{|F_t(\kappa) \cap \mathrm{A}|}{|F_t(\kappa)|}, \quad R_c(\kappa) = \frac{|F_t(\kappa) \cap \mathrm{A}_c|}{|\mathrm{A}_c|} \tag{4}$$

where $R_c(\kappa)$ is the recall for adverse class c. Precision and recall are reported at four capacities, 0.125, 0.5, 2 and 5 per cent, so that the ordering of arms can be checked across reviewer budgets. Table 3 lists every quantity the evaluation reports and its definition. All quantities are reported in full rather than selectively (Gray, 2014; Bolton, 2002).

Table 3. Quantities reported by the evaluation and their definitions.

Quantity	Definition	Reported as
Precision at capacity	Share of flagged users who are adverse, at each capacity	Per arm and capacity
Recall by class	Share of each adverse class that is flagged, at each capacity	Per arm, class and capacity

Quantity	Definition	Reported as
Register size	Number of conflicts in the register produced by each arm	Count per period
Clearable share	Share of register conflicts that documented mitigation can clear, denoted m	Proportion per arm
Remediation queue	Conflicts requiring remediation, as defined in Section 7.6	Count per arm
Reviewer time	Reviewer hours per period, as defined in Section 7.6	Hours per arm
Feature-group effect	Change in precision at the primary capacity when a feature group is removed from A4	Difference per group
Suppressor effect	Change in flag count and precision at the primary capacity when a suppressor is removed	Difference per suppressor

7.4 Adverse population classes

The adverse population has three classes, defined by the latent-conflict definition in Section 4.3. Static-conflict exploiters hold a conflict named by a rule in C and exercise both sides. Latent-conflict exploiters hold and exercise a non-segregated cycle, within one user, that no rule names. Collusive pairs are the cross-user case of a latent conflict: two users jointly complete a process without effective separation, and neither user's individual assignments are unremarkable. The protocol requires that class membership be recorded in the generator's output and that class sizes and their distribution across organizational units be reported with each study, so that recall can be read against the population on which it was measured (Brickley, 2021; Debreceny, 2010).

7.5 Feature-group ablation

The protocol eliminates each feature group from A4 one at a time and reports the change in the precision of the primary capacity. The feature groups are the authority-exercise group, the separation-bypass group, the temporal and volume group and the relational group. The suppressors are eliminated separately, both together and individually, at a fixed flag threshold to separate the effects of the suppression itself from the changes in the number of flags. Interpretation of the results of suppression is only possible when all the arms are run on the same population and with the same random seed, which is ensured by the protocol (Ominyi, 2024a; Okwesa, 2024). Suppression is performed after the comparison of the arms.

7.6 Register and reviewer-time model

Let Reg_a be the conflict register produced by arm a in a period, and let m_a be the share of its conflicts that documented mitigation can clear. The remediation queue for arm a is

$$Q_a = |\mathrm{Reg}_a| \ (1 - m_a) \tag{5}$$

For A3, which produces no register, the queue is defined over flagged users, so that $Q_{A3} = |F_t(\kappa)|$. Reviewer time is the number of queued items multiplied by the time per item, which is the sum of four task durations: reading the conflict and its evidence, confirming permissions against the platform, consulting the user or manager, and documenting the disposition.

$$H_a = \tau\ Q_a,\ \tau = \tau_{\text{read}} + \tau_{\text{confirm}} + \tau_{\text{consult}} + \tau_{\text{document}} \quad (6)$$

Each component of τ is measured in a pilot with reviewers and is reported with its variance. The durations are parameters, not results, and no total is reported for any arm until they have been measured (Aneke, 2023; Adesuyi, 2023).

7.7 Reporting requirements

For each experiment, the generator or sampling frame, the random seed, the parameter values, the class sizes, the arm definitions, and all quantities in Table 3 will be reported. Results will be reported for each capacity in the grid, even those results that are unfavorable to the architecture, along with limitations on the population underlying each result. A change in the protocol during an experiment will be reported as a deviation. These requirements apply to the synthetic and the installation-based experiments alike and are the context under which the claim about remediation economics is assessed (Trotman, 2011; Hemati, 2021). Each reported quantity will be understood in terms of its definition in Table 3 and the population over which it was measured.

8. Latent Conflicts and Multi-User Sequences

This section applies the latent-conflict definition of Section 4.3 to the two ways latent conflicts can be detected. The static way relies on the specification and works on it in a richer form. The sequential way relies on the event log and sees cross-user latent conflicts only if the activities of multiple users can be recomposed as a process instance. Two routes are needed since they detect different types of latent conflict, and Table 1 shows each mechanism and the route that detects it (Jans, 2014; van der Aalst, 2016). Neither route can get into the cross-user case without the case identifier of Section 8.2.

8.1 Detecting latent conflicts through effective capability

If the conflicts are specified over permission sets and effective permissions are calculated properly, latent conflicts arising from set equivalence and scope fragmentation become detectable by static means. The suggested specification specifies each side of the conflict as the set of permissions sufficient for the step, rather than a single permission or a role name, so that if a user has such a set on both sides, he is in static conflict regardless of the role he holds (Vaidya, 2007; Sandhu, 1996). No changes in the detection method are required. How many conflicts of this sort can be exposed is an empirical question that the protocol measures as the difference between arms A1 and A2 (Kobelsky, 2014).

8.2 Cross-user sequences and the limits of permission reasoning

Cross-user latent conflicts are the class with the biggest impact on the control, and they are the only class of conflicts that cannot be detected with tests over individual permission sets. The process instance binds the events of multiple users together, and the separation achieved within it depends on the order and the actors of the steps. The constraint is practical. ERP event logs are distributed among multiple modules, and the process instance requires a case identifier which is not maintained across these modules in the ERP system. Without the case identifier, the tier-3 features cannot be calculated and the cross-user results cannot be transferred to the installation (van der Aalst, 2016; Semi, 2024; Kanwer, 2024). The implication for practice is that the sequence layer needs to be scoped to the processes for which the case identifier is available.

9. Remediation Economics and Governance

The critical question in regard to any monitoring architecture is what happens after detection. The register whose growth outstrips the remediation capacity loses its value, and the behavioral scoring used without proper governance creates another risk for the individuals described in the scoring process. This section presents the register-growth problem and explains under what conditions behavioral scoring can increase the productivity of the remediation queue, and also presents the governance constraints on the use of scores about employees and the evidentiary standards each tier must satisfy prior to any action. The discussion follows the governance perspective of the internal-control literature (Jimoh, 2023; Stamatović, 2020). The section treats the cost of review as the primary constraint, because the design that the review function cannot accommodate does not alter control outcomes.

9.1 The register-growth trap

If detection capability improves, and remediation capacity remains constant, then the register expands. The organization can choose to increase capacity, relax the threshold for mitigation, or accept an enduring register. The former improves the control process; the latter two decrease the proportion of disputes that are solved but leave the size of the register constant. A register containing many accepted risk users is not able to distinguish between material and immaterial unmitigated disputes, and this is the reason for treating accepted risk separately (Aneke, 2023; Adesuyi, 2023).

Behavioral scoring can make the former option economically viable only if it increases productivity per hour of review. Whether it does so is an empirical issue. The model discussed in Section 7.6 formulates this issue as review time per conflict cleared under each scenario, and the protocol does not presume an answer (Okwesa, 2024; Fadayomi, 2024).

9.2 Governance of behavioral scoring on employees

Behavioral score is a proposition about the individual, and its use is circumscribed by labor law, works council agreements and data protection laws where applicable (Obriki, 2023; Onche,

2024). The two constraints are the following: purpose limitation implies that score can be used solely for access control and internal control assurance purposes, and never for performance management. Score should therefore be retained by control function, and access should be logged. Human decision requires that no action against an employee be undertaken on the basis of a score alone. Many legal jurisdictions require that, and it is a control requirement everywhere, since score is a prioritization signal, not a finding. Such governance forms part of the design, and the architecture is incomplete without it (Potla, 2024; Okwesa, 2024).

9.3 Evidentiary standards by tier

Tier-1 finding is a proposition about configuration: effective permissions of a user include conflicting access to both resources. Its accuracy depends only on the effective permission computation, which is deterministic and reproducible from the snapshot, and it is actionable per se, subject to the decision-making procedure described in Section 4.4 (Potla, 2024; Ratliff, 2022). Tier-2 finding is a statistical inference that the user's activity diverges from expectations. It requires legitimate explanation, must be reviewed before any action, and should be documented as a prioritization signal (Ominyi, 2024a; Hemati, 2021). Tier-3 finding is a reconstruction of a sequence of events and of multiple actors' actions. It is the most probative and the most sensitive type of finding, and if the finding is disputed, the reconstruction technique becomes evidence (Brickley, 2021; van der Aalst, 2016).

10. Implications

The architecture influences two groups of stakeholders, who depend on the segregation-of-duties monitoring process directly. Control functions benefit from accurate effective permission computation, and from ordering the register based on evidence of exercised authority, rather than on severity alone. Auditors treat register as the result of control process, and the relevant issues are the remediation decision, completeness of the specification, and the relation between exercised and assigned authority. The two sub-sections discuss each group separately (Hardy, 2015; Kuhn, 2010). They need the same specification to be able to test the register without access to the detection code.

10.1 For control functions

Most importantly, computing correct permissions effectively is the largest available improvement and is neither analytical nor deterministic. It is resolving composite roles, direct assignment, field value, scope and temporal validity. Those are deterministic, reproducible from the configuration snapshot, and are the building blocks of tier 1 (Sandhu, 1996; Khan, 2010). Secondly, ordering the register by evidence of exercised authority and not severity, as the latter describes what the conflict allows and the former describes what the user does. Whether the approach is better by reviewer hour is what Section 7 protocol is designed to resolve (Okwesa, 2024; Fadayomi, 2024).

10.2 For auditors

Register is not the control. An auditor must ask three questions about the control that the register cannot answer. The first is how many identified conflicts were remediated rather than mitigated or accepted, and whether the accepted population has been reviewed separately. The second question is whether the specification was validated for completeness, against process definitions, including the scope-fragmentation and cross-user cases in Table 1. The third question is whether the authority exercised is consistent with the authority assigned. The third question is answered with behavioral scoring as it pertains to whether the control works and not whether it is documented (Hardy, 2015; Trotman, 2011).

11. Conflict Specification Template

Conflict specification is as useful as its entries, but an entry lacking either the scope predicate or the sufficient permission set cannot be tested. This section offers a template for an entry and works it out in the example below. The template makes each entry testable in tier 1, records the compensating control where applicable and defines the severity on which the register ordering depends. Specification in this format also records the process steps, which are needed by tier-3 features to build instances from the event log. The example below is based on the procure-to-pay cycle, which is one of the settings in which the segregation-of-duties rules usually apply (Semi, 2024; Kobelsky, 2014). The structure of each field is explained in Section 11.1, and the example is provided in Section 11.2.

11.1 Structure

An entry in a conflict specification comprises identifier; the process step on each side; the set of permissions functionally sufficient for each step; the scope predicate; the severity rating; and the compensating control, if any. The identifier enables a conflict tracking across the versions of the register. The process step is necessary to connect the entry with the event log and enable a tier-3 feature to reference the same step. The sufficient permission set is the field without which a static test falls silent for set-equivalence conflict, and the scope predicate determines where the combination applies. Severity is the parameter used in the decision problem in Section 4.4, and it must be assigned by the control owner, not the detection system. (Kumar, 2024; Brickley, 2021).

11.2 Worked example

Take the vendor master and payment steps in the procure-to-pay cycle. Side A is vendor master maintenance, which includes sufficient permissions of the transaction codes for creation of a vendor and change of the bank details, at field level, within the relevant account group. A one-time vendor account group restriction does not provide sufficient permission for Side A. Side B is payment release. The conflict applies to a case where both sides are held for the same company code, and it is immaterial if vendor master maintenance is restricted to a company code in which the user does not have payment authority. The user holding Side A for company code 1000 and Side B for company code 2000 is thus not in static conflict, despite the procure-to-pay

process covering both company codes and user's being a candidate for scope-fragmentation latent conflict (Semi, 2024; Brickley, 2021).

12. Conclusion

SOD monitoring in ERP software is a well-established control with two fundamental weaknesses in its structure. A static matrix generates a register that is a function of the definition rather than the risk level, and it does not capture conflicts arising out of a combination of permissions or from sequences of actions. In this paper, the architecture that overcomes both of those challenges without changing the role of the matrix as the authority for conflict detection is defined. Conflicts are first defined once, the remediation problem is formalized and an evaluation protocol is stated that does not reveal any result of empirical significance. The question of whether this architecture makes a difference to the economics of remediation is for the protocol to decide. The most difficult case of user collusion, in which individual user behavior shows nothing unusual, has been addressed only by the sequence layer under conditions of a case identifier being present.

References

This paper cites 200 references: 100 drawn from the client reference library provided for this project, and 100 discovered in the author's own research. All entries are dated 2024 or earlier, the cut-off date used in the title of this paper.

1. Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2022). Real-time compliance pipelines: A review of automated risk monitoring and enterprise data governance. International Journal of Multidisciplinary Futuristic Development, 3(2), 66-94. https://doi.org/10.54660/IJMFD.2022.3.2.66-94
2. Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2022). Real-time compliance pipelines: A review of automated risk monitoring and enterprise data governance. International Journal of Multidisciplinary Futuristic Development, 3(2), 66-94. https://doi.org/10.54660/IJMFD.2022.3.2.66-94
3. Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., & Akeju, B. (2021). Conceptual model for identity-centric Zero Trust Architecture in enterprise security governance. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(5), 393–415. https://doi.org/10.32628/IJSRCSEIT
4. Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., & Akeju, B. (2021). Conceptual model for identity-centric zero trust architecture in enterprise security governance. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(5), 393-415. https://doi.org/10.32628/IJSRCSEIT217562
5. Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., & Akeju, B. (2021). Conceptual model for identity-centric zero trust architecture in enterprise security

governance. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(5), 393-415. https://doi.org/10.32628/IJSRCSEIT217562

6. Dosunmu, A. A., & Ogundele, P. O. (2019). Security audit and enterprise risk assessment frameworks for resilient information systems. Iconic Research and Engineering Journals, 3(5), 434-447. https://doi.org/10.64388/IREV3I5-1713225
7. Dosunmu, A. A., & Ogundele, P. O. (2019). Security audit and enterprise risk assessment frameworks for resilient information systems. Iconic Research and Engineering Journals, 3(5), 434-447. https://doi.org/10.64388/IREV3I5-1713225
8. Bello, A. D., Elebe, O., Hammed, N. I., Omoegun, G. O., & Fadayomi, O. (2024). A cybersecurity risk management and regulatory compliance framework for financial institutions. Iconic Research and Engineering Journals. https://www.irejournals.com/paper-details/1713553
9. Bello, A. D., Elebe, O., Hammed, N. I., Omoegun, G. O., & Fadayomi, O. (2024). Cybersecurity risk management and regulatory compliance framework for financial institutions. Iconic Research and Engineering Journals. https://www.irejournals.com/paper-details/1713553
10. Dosunmu, A. A., & Ogundele, P. O. (2024b). Cyber risk quantification models for prioritizing enterprise security investment decisions. International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), 1777-1785. https://doi.org/10.54660/.IJMRGE.2024.5.6.1777-1785
11. Dosunmu, A. A., & Ogundele, P. O. (2024b). Cyber risk quantification models for prioritizing enterprise security investment decisions. International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), 1777-1785. https://doi.org/10.54660/.IJMRGE.2024.5.6.1777-1785
12. Okafor, C. M., Osuji, V. C., & Dako, O. F. (2024). Harmonizing risk governance, technology infrastructure, and compliance frameworks for future-ready banking systems. International Journal of Scientific Research in Humanities and Social Sciences, 1(1), 316-337.
13. Okafor, C. M., Osuji, V. C., & Dako, O. F. (2024). Harmonizing risk governance, technology infrastructure, and compliance frameworks for future-ready banking systems. International Journal of Scientific Research in Humanities and Social Sciences, 1(1), 316-337.
14. Ebhojie, O., Dogbatsey, E. A., & Oyeleye, A. O. (2023a). Audit liaison, corrective action planning, and control compliance in multinational organizations: A systematic literature review. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2839-2850. https://doi.org/10.62225/2583049X.2023.3.6.6200
15. Ebhojie, O., Dogbatsey, E. A., & Oyeleye, A. O. (2023a). Audit liaison, corrective action planning, and control compliance in multinational organizations: A systematic literature review. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2839-2850. https://doi.org/10.62225/2583049X.2023.3.6.6200
16. Feboh, D., Ijagbemi, A. O., Nwakamma, S., Izuchukwu, O. T., & Oyefuga, M. (2023). Cybersecurity governance in smart campus environments: Balancing ISO 27001, GDPR, and

HIPAA compliance in university IT systems. International Journal of Multidisciplinary Research and Growth Evaluation, 4(6), 1619–1631. https://doi.org/10.54660/.IJMRGE.2023.4.6.1619-1631

17. Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2023b). Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2890-2904. https://doi.org/10.62225/2583049X.2023.3.6.6206
18. Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2023b). Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2890-2904. https://doi.org/10.62225/2583049X.2023.3.6.6206
19. Mbonu, I.S., Iwuanyanwu, U., Aliliele, C. & Uzoka, E., 2022. Advances in Cloud Identity and Access Governance Optimization in Large Scale AWS Enterprise Environments. Shodhshauryam, International Scientific Refereed Research Journal, 5(3), pp.403–438. DOI: 10.32628/SHISRRJ225490.
20. Peteranaba, S. F., Osinem, H. E., Eribenne, F., & Soyege, O. S. (2022). Health information governance and regulatory compliance: Comparative frameworks for data verification, risk screening, and confidentiality in health and financial systems. International Journal of Science, Technology & Society, 6(1), 60-84.
21. Peteranaba, S. F., Osinem, H. E., Eribenne, F., & Soyege, O. S. (2022). Health information governance and regulatory compliance: Comparative frameworks for data verification, risk screening, and confidentiality in health and financial systems. International Journal of Science, Technology & Society, 6(1), 60-84.
22. Peteranaba, S. F., Osinem, H. E., Eribenne, F., & Soyege, O. S. (2022). Health information governance and regulatory compliance: Comparative frameworks for data verification, risk screening, and confidentiality in health and financial systems. International Journal of Science, Technology & Society, 6(1), 60-84.
23. Mbonu, I.S., Iwuanyanwu, U., Aliliele, C. & Uzoka, E., 2020. A Conceptual Framework for Agile Supply Chain Digital Transformation with Embedded IT Risk and ISO Compliance Controls. Iconic Research and Engineering Journals, 3(11), pp.566–593. DOI: 10.64388/IREV3I11-1714916.
24. Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Oluoha, O. M. (2018). A conceptual framework for legal and ethical risk modeling in enterprise data protection governance systems. Iconic Research and Engineering Journals, 2(2), 207-226. https://doi.org/10.64388/IREV2I2-1714911
25. Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Oluoha, O. M. (2018). A conceptual framework for legal and ethical risk modeling in enterprise data protection governance systems. Iconic Research and Engineering Journals, 2(2), 207-226. https://doi.org/10.64388/IREV2I2-1714911

26. Mbonu, I.S., Aliliele, C., Iwuanyanwu, U. & Oluoha, O.M., 2018. A Conceptual Framework for Legal and Ethical Risk Modeling in Enterprise Data Protection Governance Systems. Iconic Research and Engineering Journals, 2(2), pp.207–226. DOI: 10.64388/IREV2I2-1714911.
27. Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2024b). An AI driven security operations architecture for utility sector SOCs: Integrating threat intelligence, behavioral analytics, and automated response. International Journal of Engineering and Modern Technology, 10(11), 197-256. https://doi.org/10.56201/ijemt.v10.no11.2024.pg197.256
28. Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2024b). An AI driven security operations architecture for utility sector SOCs: Integrating threat intelligence, behavioral analytics, and automated response. International Journal of Engineering and Modern Technology, 10(11), 197-256. https://doi.org/10.56201/ijemt.v10.no11.2024.pg197.256
29. Aliliele, C., Eboh, E. E., & Oluwo, K. (2024). Advances in variance analytics for cost control in manufacturing and industrial enterprises. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3163-3185. https://doi.org/10.62225/2583049X.2024.4.6.6012
30. Aliliele, C., Eboh, E. E., & Oluwo, K. (2024). Advances in variance analytics for cost control in manufacturing and industrial enterprises. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3163-3185. https://doi.org/10.62225/2583049X.2024.4.6.6012
31. Aliliele, C., Eboh, E. E., & Oluwo, K. (2024). Advances in variance analytics for cost control in manufacturing and industrial enterprises. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3163-3185. https://doi.org/10.62225/2583049X.2024.4.6.6012
32. Amarahobu, C., Uwagboe, F.-M., & Ojeakhena, F. (2024). Outsourced security in Nigeria's oil and gas sector: Contractor selection, performance monitoring and cost control. International Journal of Science, Technology and Society, 8(1), 201–223.
33. Ashore-Onisemo, F., Iziduh, E. F., Unamma, U. M.-L., & Okwesa, I. J. (2024). Bridging legal, financial, and data governance in enterprise AI: Emerging trends. International Journal of Economics and Financial Management, 9(9), 336-381. https://doi.org/10.56201/ijefm.v9.no9.2024.pg336.381
34. Ashore-Onisemo, F., Iziduh, E.F., Unamma, U.M.-L. & Okwesa, I.J., 2024. Legal-Financial-Data Governance of Enterprise AI: New Directions. International Journal of Economics and Financial Management, 9(9), pp.336-381. DOI: 10.56201/ijefm.v9.no9.2024.pg336.381
35. Badmus, O., Jooda, D., & Anunagba, C. O. (2024). A privacy-by-design framework for role-based security architecture in Salesforce environments handling sensitive personal data. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3244-3254. https://doi.org/10.62225/2583049X.2024.4.6.6243
36. Badmus, O., Jooda, D., & Anunagba, C. O. (2024). A privacy-by-design framework for role-based security architecture in Salesforce environments handling sensitive personal data.

International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3244-3254. https://doi.org/10.62225/2583049X.2024.4.6.6243

37. Eboh, E. E., & Aliliele, C. (2024). AI-driven data analytics framework for risk assessment and detection of venture capital and private equity investment fraud in U.S. capital markets. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(6), 2624-2665. https://doi.org/10.32628/CSEIT2410787
38. Eboh, E. E., & Aliliele, C. (2024). AI-driven data analytics framework for risk assessment and detection of venture capital and private equity investment fraud in U.S. capital markets. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(6), 2624-2665. https://doi.org/10.32628/CSEIT2410787
39. Eboh, E.E. & Aliliele, C., 2024. AI-Driven Data Analytics Framework for Risk Assessment and Detection of Venture Capital and Private Equity Investment Fraud in U.S. Capital Markets. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(6), pp.2624–2665. DOI: 10.32628/CSEIT2410787.
40. Fadayomi, O., Bello, A. D., Elebe, O., Hammed, N. I., & Omoegun, G. O. (2024). An adaptive fraud risk scoring model for real-time transaction monitoring at scale. IIARD International Journal of Banking and Finance Research, 10(10), 212-230.
41. Fadayomi, O., Bello, A. D., Elebe, O., Hammed, N. I., & Omoegun, G. O. (2024). An adaptive fraud risk scoring model for real-time transaction monitoring at scale. IIARD International Journal of Banking and Finance Research, 10(10), 212-230.
42. Fadero, S., Abdulwahab, A. I., Minoungou, T. F. T., Anene, U., & Kumuyi, O. (2024). Risk based testing in complex enterprise systems. International Journal of Humanities and Information Technology, 6(4), 275–311.
43. Falemi, A., Akhigbe, R., & Akin-Oluyomi, O. T. (2024). A conceptual enterprise risk management model that integrates HR strategy with operational analytics. International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), 1730-1753. https://doi.org/10.54660/.ijmrge.2024.5.6.1730-1753
44. Falemi, A., Akhigbe, R., & Akin-Oluyomi, O. T. (2024). An enterprise risk management framework that integrates human resource strategy and operational analytics. International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), 1730-1753. https://doi.org/10.54660/.ijmrge.2024.5.6.1730-1753
45. Okafor, C. M., Farounbi, B. O., Adesanya, O. S., & Akinola, A. S. (2024). Controls for cross-border payments operations: Correspondent banking risk reduction through end-to-end monitoring. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(4), 1050-1071.
46. Okafor, C. M., Farounbi, B. O., Adesanya, O. S., & Akinola, A. S. (2024). Controls for cross-border payments operations: Correspondent banking risk reduction through end-to-end monitoring. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(4), 1050-1071.

47. Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., & Akeju, B. (2024). Trends in enterprise cybersecurity and evolving threats: Advances and new directions for research. Global Multidisciplinary Perspectives Journal, 1(6), 194-204. https://doi.org/10.54660/GMPJ.2024.1.6.194-204
48. Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., & Akeju, B. (2024). Trends in enterprise cybersecurity and evolving threats: Advances and new directions for research. Global Multidisciplinary Perspectives Journal, 1(6), 194-204. https://doi.org/10.54660/GMPJ.2024.1.6.194-204
49. Okwesa, I. J., Ashore-Onisemo, F., Oyesiji, S. O., & Abdulmalik, A. U. (2024). Predictive risk analytics for early-warning systems in enterprise technology estates. Shodhshauryam, International Scientific Refereed Research Journal, 7(6), 327-386. https://doi.org/10.32628/SHISRRJ24797 [Verify pages: the article running header reads 318-326.]
50. Okwesa, I. J., Ashore-Onisemo, F., Oyesiji, S. O., & Abdulmalik, A. U. (2024). Predictive risk analytics for early-warning systems in enterprise technology estates. Shodhshauryam, International Scientific Refereed Research Journal, 7(6), 327-386. https://doi.org/10.32628/SHISRRJ24797 [Verify pages: the article running header reads 318-326.]
51. Okwesa, I.J., Ashore-Onisemo, F., Oyesiji, S.O. & Abdulmalik, A.U., 2024. Predictive Risk Analytics for Early-Warning Systems in Enterprise Technology Estates. Shodhshauryam, International Scientific Refereed Research Journal, 7(6), pp.327–386. DOI: 10.32628/SHISRRJ24797.
52. Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2024a). Developing a conceptual framework for AI-assisted compliance monitoring and anomaly detection in high-volume transaction environments. World Journal of Innovation and Modern Technology, 8(6), 204-228. https://doi.org/10.56201/wjimt.v8.no6.2024.pg204.228
53. Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2024a). Developing a conceptual framework for AI-assisted compliance monitoring and anomaly detection in high-volume transaction environments. World Journal of Innovation and Modern Technology, 8(6), 204-228. https://doi.org/10.56201/wjimt.v8.no6.2024.pg204.228
54. Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2024). Effectiveness of cybersecurity awareness training on insider-threat behavior among university administrators: An integrative academic review. International Journal of Computer Science and Mathematical Theory, 10(2), 117-144. https://doi.org/10.56201/ijcsmt.v10.no2.2024.pg117.144 Ayinde, M., Ojukwu, P. U., & Ohunyon, G. (2023). Enhancing patient safety in clinical decision units through nurse-led quality improvement. International Journal of Multidisciplinary Research and Growth Evaluation, 4(6), 1478-1491. https://doi.org/10.54660/.IJMRGE.2023.4.6.1478-1491
55. Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2024). Effectiveness of cybersecurity awareness training on insider-threat behavior among university administrators: An

integrative academic review. International Journal of Computer Science and Mathematical Theory, 10(2), 117-144. https://doi.org/10.56201/ijcsmt.v10.no2.2024.pg117.144

56. Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2024). Effectiveness of cybersecurity awareness training on insider-threat behavior among university administrators: An integrative academic review. International Journal of Computer Science and Mathematical Theory, 10(2), 117-144. https://doi.org/10.56201/ijcsmt.v10.no2.2024.pg117.144
57. Unamma, U. M.-L., Okwesa, I. J., Oyesiji, S. O., & Abdulmalik, A. U. (2024). Identity and access governance in hybrid cloud environments: Advances and future directions. Gyanshauryam, International Scientific Refereed Research Journal, 7(3), 383-430. https://doi.org/10.32628/GISRRJ247328
58. Unamma, U.M-L., Okwesa, I.J., Oyesiji, S.O. & Abdulmalik, A.U., 2024. Identity and Access Governance in Hybrid Cloud Environments: Advances and Future Directions. Gyanshauryam, International Scientific Refereed Research Journal, 7(3), pp.383–430. DOI: 10.32628/GISRRJ247328
59. Adebayo, A., Adegbite, M. P., & Ahmed, M. O. (2023). AI augmented threat detection in industrial control systems: A systematic review of machine learning approaches for ICS anomaly detection. International Journal of Engineering and Modern Technology, 9(3), 287-340. https://doi.org/10.56201/ijcsmt.v9.no3.2023.pg287.340
60. Adebayo, A., Adegbite, M. P., & Ahmed, M. O. (2023). AI augmented threat detection in industrial control systems: A systematic review of machine learning approaches for ICS anomaly detection. International Journal of Engineering and Modern Technology, 9(3), 287-340. https://doi.org/10.56201/ijcsmt.v9.no3.2023.pg287.340
61. Adelanwa, A., Basnet, A., & Anene, U. N. (2023b). Predictive analytics models for financial risk detection and fraud prevention in public systems. International Journal of Advanced Multidisciplinary Research and Studies, 3(6). https://doi.org/10.62225/2583049X.2023.3.6.5969
62. Adelanwa, A., Basnet, A., & Anene, U. N. (2023b). Predictive analytics models for financial risk detection and fraud prevention in public systems. International Journal of Advanced Multidisciplinary Research and Studies, 3(6). https://doi.org/10.62225/2583049X.2023.3.6.5969
63. Adeniji, E. H., Owhonda, K. C., Stephen-Kings, G., & Ohikhuare, J. (2023). Leveraging enterprise analytics to align risk mitigation, health IT deployment, and continuous clinical process improvement. International Journal of Science and Research Archive, 10(2), 1314-1329. https://doi.org/10.30574/ijsra.2023.10.2.1003
64. Adeniji, E.H., Owhonda, K.C., Stephen-Kings, G. & Ohikhuare, J., 2023. Utilizing Enterprise Analytics to Align Risk Management, Implementation of Health IT, and Clinical Process Improvement. International Journal of Science and Research Archive, 10(2), pp.1314–1329. DOI: 10.30574/ijsra.2023.10.2.1003.
65. Adesuyi, M. O., Kalu, A., & Walawalkar, G. (2023). Data-driven cost governance in technology-intensive firms. International Journal of Scientific Research in Computer

Science, Engineering and Information Technology, 9(3), 877–896. https://doi.org/10.32628/IJSRCSEIT

66. Adesuyi, M. O., Kalu, A., & Walawalkar, G. (2023). Data-driven cost governance in technology-intensive firms. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(3), 877-896. https://doi.org/10.32628/IJSRCSEIT
67. Adesuyi, M. O., Kalu, A., & Walawalkar, G. (2023). Data-driven cost governance in technology-intensive firms. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(3), 877-896. https://doi.org/10.32628/IJSRCSEIT
68. Adeyelu, O. O. (2023). Risk-based model for oversight of unmanned aerial vehicle operations in shared controlled airspace above Nigerian airports. International Journal of Scientific Research in Civil Engineering, 7(4), 147-184. https://doi.org/10.32628/IJSRCE237419
69. Adeyelu, O. O. (2023). A risk-tiered oversight model for unmanned aircraft operations in shared controlled airspace over Nigerian airports. International Journal of Scientific Research in Civil Engineering, 7(4), 147-184. https://doi.org/10.32628/IJSRCE237419
70. Adeyelu, O.O., 2023. A Risk-Tiered Oversight Model for Unmanned Aircraft Operations in Shared Controlled Airspace Over Nigerian Airports. International Journal of Scientific Research in Civil Engineering, 7(4), pp.147–184. DOI: 10.32628/IJSRCE237419.
71. Agu, M. U., Akomolafe, O., & Bello, A. (2023a). A comparative review of SOX compliance frameworks in cross-border financial auditing. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2297-2306. https://doi.org/10.62225/2583049X.2023.3.6.5362
72. Agu, M. U., Akomolafe, O., & Bello, A. (2023a). A comparative review of SOX compliance frameworks in cross-border financial auditing. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2297-2306. https://doi.org/10.62225/2583049X.2023.3.6.5362
73. Akomolafe, O., Agu, M. U., & Bello, A. (2023a). A conceptual model for implementing risk-based auditing in strategic financial management. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2274-2286. https://doi.org/10.62225/2583049X.2023.3.6.5359
74. Akomolafe, O., Agu, M. U., & Bello, A. (2023b). A quantitative conceptual model for assessing compliance risk in emerging economies. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2287-2296. https://doi.org/10.62225/2583049X.2023.3.6.5360
75. Akomolafe, O., Agu, M. U., & Bello, A. (2023a). A conceptual model for implementing risk-based auditing in strategic financial management. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2274-2286. https://doi.org/10.62225/2583049X.2023.3.6.5359

76. Akomolafe, O., Agu, M. U., & Bello, A. (2023b). A quantitative conceptual model for assessing compliance risk in emerging economies. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2287-2296. https://doi.org/10.62225/2583049X.2023.3.6.5360
77. Aliliele, C., Mbonu, I.S. & Iwuanyanwu, U., 2023. A Conceptual Framework for Continuous Cloud Misconfiguration Monitoring and Enterprise Risk Mitigation Strategies. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(10), pp.373-394. DOI: 10.32628/CSEIT2361071.
78. Aliliele, C., Mbonu, I.S. & Iwuanyanwu, U., 2023. A Review of API Governance and Risk Prioritization Frameworks in Modern Financial Institutions. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(10), pp.395-433. DOI: 10.32628/CSEIT2361072.
79. Amarahobu, C., Uwagboe, F.-M., & Ojeakhena, F. (2023). Analog to IP migration: Lessons from large scale CCTV and access control systems implementation in Nigerian corporate buildings. International Journal of Technology Management & Humanities, 9(4), 482–503. https://doi.org/10.21590/ijtmh.09.04.34
80. Amayo, E. B., Owulade, O. A., & Isi, L. R. (2023b). Risk management strategies and compliance frameworks in health care infrastructure projects: Case study of projects in West Africa. International Journal of Management and Organizational Research, 2(1), 161-168. https://doi.org/10.54660/IJMOR.2023.2.1.161-168
81. Amayo, E. B., Owulade, O. A., & Isi, L. R. (2023b). Risk management strategies and compliance frameworks in health care infrastructure projects: Case study of projects in West Africa. International Journal of Management and Organizational Research, 2(1), 161-168. https://doi.org/10.54660/IJMOR.2023.2.1.161-168
82. Aneke, O. B., Sydney, E., & Adesemoye, A. C. (2023). Data Integrity and Governance in Regulated Life Sciences Operations: Review of Failures, Controls, and Remediation Strategies. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(10), 538-568.
83. Aneke, O. B., Sydney, E., & Adesemoye, A. C. (2023). Data Integrity and Governance in Regulated Life Sciences Operations: Review of Failures, Controls, and Remediation Strategies. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(10), 538-568.
84. Aneke, O.B., Sydney, E. & Adesemoye, A.C., 2023. Data Integrity and Governance in Regulated Life Sciences Operations: A Review of Failures, Controls, and Remediation Strategies. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(10), pp.538–568.
85. Bello, A., Akomolafe, O., & Agu, M. U. (2023). A conceptual framework for data-driven procurement risk management in multinational enterprises. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2307-2316. https://doi.org/10.62225/2583049X.2023.3.6.5363

86. Bello, A., Akomolafe, O., & Agu, M. U. (2023). A conceptual framework for data-driven procurement risk management in multinational enterprises. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2307-2316. https://doi.org/10.62225/2583049X.2023.3.6.5363
87. Dosunmu, A. A., & Ogundele, P. O. (2023). Cyber threat actor analysis models for strategic enterprise security planning. Shodhshauryam, International Scientific Refereed Research Journal, 6(5), 513-531.
88. Dosunmu, A. A., & Ogundele, P. O. (2023). Cyber threat actor analysis models for strategic enterprise security planning. Shodhshauryam, International Scientific Refereed Research Journal, 6(5), 513-531.
89. Eboh, E. E., & Aliliele, C. (2023). Portfolio risk optimization models for venture capital investment strategy and fraud exposure analysis. Iconic Research and Engineering Journals, 7(4), 759-792. https://doi.org/10.64388/IREV7I4-1715305
90. Eboh, E. E., & Aliliele, C. (2023). Portfolio risk optimization models for venture capital investment strategy and fraud exposure analysis. Iconic Research and Engineering Journals, 7(4), 759-792. https://doi.org/10.64388/IREV7I4-1715305
91. Eboh, E.E. & Aliliele, C., 2023. Portfolio Risk Optimization Models for Venture Capital Investment Strategy and Fraud Exposure Analysis. Iconic Research and Engineering Journals, 7(4), pp.759–792. DOI: 10.64388/IREV7I4-1715305.
92. Elebe, O., Hammed, N. I., Omoegun, G. O., Fadayomi, O., & Bello, A. D. (2023). An advanced machine learning model for detecting synthetic identity fraud in e-commerce platforms [Preprint]. ResearchGate.
93. Elebe, O., Hammed, N. I., Omoegun, G. O., Fadayomi, O., & Bello, A. D. (2023). An advanced machine learning model for detecting synthetic identity fraud in e-commerce platforms [Preprint]. ResearchGate.
94. Eze, F. I., Anene, U. N., & Akinleye, O. K. (2023). Pharmaceutical supply chain governance, environmental risk management, and sustainable access to essential medicines in emerging economies: The PSCG-ERM framework. International Journal of Health and Pharmaceutical Research, 8(4), 192-241. https://doi.org/10.56201/ijhpr.v8.no4.2023.pg192.241
95. Eze, F. I., Anene, U. N., & Akinleye, O. K. (2023). Pharmaceutical supply chain governance, environmental risk management, and sustainable access to essential medicines in emerging economies: The PSCG-ERM framework. International Journal of Health and Pharmaceutical Research, 8(4), 192-241. https://doi.org/10.56201/ijhpr.v8.no4.2023.pg192.241
96. Jimoh, H. O., Ahmed, M. O., & Fagbade, M. O. (2023). The role of frameworks in cybersecurity governance. Journal of Behavioural Informatics, Digital Humanities and Development Research, 9(4), 7-16. https://doi.org/10.22624/AIMS/BHI/V9N4P2
97. Jimoh, H. O., Ahmed, M. O., & Fagbade, M. O. (2023). The role of frameworks in cybersecurity governance. Journal of Behavioural Informatics, Digital Humanities and Development Research, 9(4), 7-16. https://doi.org/10.22624/AIMS/BHI/V9N4P2

98. Jones, B. C., & Ominyi, M. (2023). Reviewing compliance frameworks for technology transfers between developed and emerging markets in an era of export controls and sanctions. World Journal of Innovation and Modern Technology, 7(2), 121-149. https://doi.org/10.56201/wjimt.v7.no2.2023.pg121.149
99. Jones, B. C., & Ominyi, M. (2023). Review of technology transfer compliance frameworks between developed and emerging markets in the era of export controls and sanctions. World Journal of Innovation and Modern Technology, 7(2), 121-149. https://doi.org/10.56201/wjimt.v7.no2.2023.pg121.149
100. Obriki, O. D., Obogo, S. F., & Arumosoye, O. M. (2023). Review of behavioral safety program as a tool for risk reduction in large organizations. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2760-2775. https://doi.org/10.62225/2583049X.2023.3.6.6076
101. Navandar, P. (2024). Governance, Risk, and Compliance (GRC) in the Age of Identity and Access Governance (IAG). International Journal of Research and Applied Sciences, 3(4).
102. Potla, R. B. (2024). A SOX/ITAR-Compliant Global ERP Template for Multi-Plant Manufacturers: Governance Patterns and Controls. Journal of Artificial Intelligence, Machine Learning and Data Science, 2(1).
103. Gonçalves, R. C. M. G., & Imoniana, J. O. (2022). Low complexity ERP readiness for continuous auditing in SMEs: The case of Brazil. Control and Cybernetics, 51(3).
104. Brickley, J. C., & Thakur, K. (2021). Least privilege and segregation of duties policy, their implementation, application and effectiveness. International Journal of Cyber Security and Digital Forensics, 10(1), 1-19.
105. Trotman, K. T., & Wright, A. (2011). Triangulation of audit evidence in fraud risk assessments. Accounting, Organizations and Society, 37(1), 41-53.
106. Proctor, P. E., Heiser, J., & MacDonald, N. (2007). MarketScope for segregation of duties controls within ERP. Gartner Research Report R2183.
107. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-Based Access Control Models. IEEE Computer, 29(2), 38-47.
108. Jalagam, R., Allu, S., Kuraku, S., & Shrivastava, N. (2024). Explainable AI based frameworks for enterprise reporting anomalies attribution. Journal of Emerging Intelligence Technologies, 2(1).
109. Kanwer, B. (2024). AI-enabled process mining and security validation of business processes on SAP S/4HANA Cloud to modernize enterprises. International Journal of Engineering & Extended Technologies, 2(4).
110. Péter, B. Z., & Kocsis, I. (2024). Private non-interactive compliance audits of blockchains using zero-knowledge proofs. Acta Polytechnica Hungarica, 21(7).
111. Rahman, M. (2024). Detection of anomalies and process mining of financial irregularities to improve procurement controls. American Journal of Advanced Technology and Science, 1(1).

112. Ratliff, T. (2022). Internal control techniques for enterprise resource planning systems. Walden University.
113. Hemati, H., Schreyer, M., & Borth, D. (2021). Continual learning approaches to unsupervised anomaly detection for continuous audit of financial accounting records. arXiv preprint arXiv:2112.13215.
114. Stamatović, M., & Maksimović, S. (2020). Risk management as part of the internal financial controls system: Implementation in the public sector of Serbia. Economy and Market Communication Review, 10(2).
115. Lopez, J., & Rubio, J. E. (2018). Access control for cyber-physical systems interconnected to the cloud. Computer Networks, 134, 46-54.
116. Gray, G. L., & Debreceny, R. S. (2014). A taxonomy to guide research on the use of data mining to detect fraud during financial statement audits. International Journal of Accounting Information Systems, 15(4), 357–380.
117. Curtis, M. B., & Turley, S. (2012). The business risk audit: A longitudinal field study of an audit engagement. Accounting, Organizations and Society, 37(7), 439-460.
118. Nigrini, M. J. (2012). Benford's Law: Applications for forensic accounting, auditing, and fraud detection. Wiley.
119. Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. Auditing: A Journal of Practice & Theory, 30(2), 19-50.
120. Jans, M., Lybaert, N., & Vanhoof, K. (2010). Internal fraud risk reduction: Results of a data mining case study. International Journal of Accounting Information Systems, 11(1), 17-41.
121. Khan, R., Corney, M., Clark, A., & Mohay, G. (2010). Transaction mining for fraud detection in ERP systems. Information Systems Management, 27(2), 141-156.
122. Kuhn, J. R., & Sutton, S. G. (2010). Continuous auditing in ERP system environments: The current state and future directions. Journal of Information Systems, 24(1), 91-112.
123. Singleton, T. W., & Singleton, A. J. (2010). Fraud Auditing and Forensic Accounting (4th ed.). Wiley.
124. Khan, R., Corney, M., Clark, A., & Mohay, G. (2009). Role mining inspired approach for modeling user behavior in ERP systems. Proceedings of the Asia Pacific Management Conference, 14, 1–12.
125. Vaidya, J., Atluri, V., & Warner, J. (2007). Role mining problem: Finding a minimal descriptive set of roles. Proceedings of the 12th ACM Symposium on Access Control Models and Technologies, 175–184.
126. Bell, T. B., & Carcello, J. V. (2000). A decision aid for assessing the likelihood of fraudulent financial reporting. Auditing: A Journal of Practice & Theory, 19(1), 169–184.
127. Gilbert, C., & Gilbert, M. A. (2024). The incorporation of blockchain technology in database management systems for improved security and transparency. International Journal of Advanced Engineering and Science, 9(2).

128. Kumar, M., & Vaitinadin, M. (2024). AI-based invoicing process in ERP systems: Reference architecture for confidence-based touchless accounts payable automation. International Journal of Scientific Research in Engineering and Management, 8(9).
129. Maas, A. (2024). Process Mining for digital audit: Flaws of existing process mining approaches as tools for data-based audit of financial statements. University of Duisburg-Essen.
130. Braim, S. J., & Mohammed, R. B. (2023). COSO framework: The influence of the components of internal control on the operations of manufacturing firms. Qalaai Zanist Scientific Journal, 8(2).
131. LoCurto, J. J. (2023). Medicare Advantage? If you say so: Waste, fraud, and abuse in Medicare Part C. Journal of Healthcare Ethics & Administration, 9(1).
132. Shovon, M. A. C., & Pal, T. (2022). An empirical investigation into the effect of robotic process automation and continuous auditing on the quality of financial report assurance. International Journal of Business and Economics Insights, 1(1).
133. Gierbl, A. S. (2021). Data analytics in external auditing. University of St. Gallen.
134. Chen, Z. X., Hohmann, L., Banjara, B., & Zhao, Y. (2020). Recommendations to safeguard patients and health care practices from Medicare and Medicaid fraud. Journal of the American Pharmacists Association, 60(4), e1–e8.
135. Adeyemi, F. K., & Olarewaju, O. M. (2019). Internal control system and financial accountability: Investigation of the South-Western Nigeria public sector. Acta Universitatis Danubius: Oeconomica, 15(1), 45–62.
136. Hamdan, K. H. (2019). Application of COSO internal control framework in evaluating disaster management in Iraq. Muthanna Journal of Administrative and Economic Sciences, 9(2).
137. Ujkani, S., & Vokshi, N. B. (2019). Development of internal controls within public sector organizations: Evidence from Kosovo. University of Malta.
138. Gonzalez, G. C., & Hoffman, V. B. (2018). Impact on the auditee of electronic vs. face-to-face contact in continuous auditing. Journal of Forensic & Investigative Accounting, 10(1), 92–110.
139. Kogan, A., Alles, M. G., & Vasarhelyi, M. A. (2018). External auditing analytical procedures: Literature survey and framework for external audit analytics. Journal of Accounting Literature, 40, 83-101.
140. Moffitt, K. C., Rozario, A. M., & Vasarhelyi, M. A. (2018). Robotic process automation in auditing. Journal of Emerging Technologies in Accounting, 15(1), 1-10.
141. Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. Auditing: A Journal of Practice & Theory, 36(4), 1-27.
142. Kirk, K. M. (2017). A predictive model analysis of Medicare and Medicaid inpatient stays and the recovery audit contracting program. Rutgers University.

143. Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. Advances in Neural Information Processing Systems, 30, 4765–4774.
144. Mohammed, M. A. (2017). Proposed framework for the design, implementation and execution of an effective internal control system. Ankara Yıldırım Beyazıt University.
145. Alles, M., & Gray, G. L. (2016). Incorporation of big data into audits: Identification of inhibitors and research agenda to overcome the inhibitors. International Journal of Accounting Information Systems, 22, 44-59.
146. Issa, H., Ting, S., & Vasarhelyi, M. A. (2016). Research suggestions for AI in auditing: Formalization and augmentation of audit process and workforce. Journal of Emerging Technologies in Accounting, 13(2), 1-20.
147. Kiesow, A., Schomaker, T., & Thomas, O. (2016). Implementation of continuous auditing in the digital era: Knowledge base from three decades of research. Proceedings of the European Conference on Information Systems.
148. Lee, H. C. (2016). Can electronic tax invoicing promote tax compliance? Evidence from electronic tax invoicing for value-added tax in the Republic of Korea. World Bank Policy Research Working Paper 7592.
149. Akoglu, L., Tong, H., & Koutra, D. (2015). Graph based anomaly detection and description: A survey. Data Mining and Knowledge Discovery, 29(3), 626–688.
150. Alles, M. G. (2015). Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession. Accounting Horizons, 29(2), 439–449.
151. Hardy, C. A., & Laslett, G. (2015). Continuous auditing and monitoring in practice: Lessons from Metcash's business assurance group. Journal of Information Systems, 29(2), 183-194.
152. King, K. M. (2015). Medicare Part D: Changes needed to improve CMS's recovery audit program operations and contractor oversight (GAO-15-633). U.S. Government Accountability Office.
153. Wang, T., & Cuthbertson, R. (2015). Eight issues on audit data analytics we would like researched. Journal of Information Systems, 29(1), 155–162.
154. Chiu, V. (2014). Development and Intellectual Structure of Continuous Auditing Research. Journal of Accounting Literature, 33, 37–57.
155. Haney, C., & Phelps, D. (2014). Responding to CMS Overpayment Demands: Practical Steps for an Appeal. The Health Lawyer, 26(6), 21–28.
156. Jans, M., van der Werf, J. M., Lybaert, N., & Vanhoof, K. (2014). Business Process Mining Application for Internal Transaction Fraud Mitigation. Expert Systems with Applications, 38(10), 13351-13359.
157. Kobelsky, K. (2014). Segregation of Duties Conceptual Model: Integrating Theory and Practice for Manual and IT-Based Processes. International Journal of Accounting Information Systems, 15(4), 300-311.

158. Kogan, A., Alles, M. G., Vasarhelyi, M. A., & Wu, J. (2014). Design and Evaluation of a Continuous Data Level Auditing System. Auditing: A Journal of Practice & Theory, 33(4), 221–245.
159. Babatunde, S. A. (2013). Perceptions of stakeholders on the effectiveness of the internal control system on financial accountability in Nigeria's public sector. International Journal of Business and Management Invention, 2(1), 16-33.
160. Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal Control—Integrated Framework. COSO.
161. Jans, M., Alles, M. G., & Vasarhelyi, M. A. (2013). The case for process mining in auditing: Sources of value added and areas of application. International Journal of Accounting Information Systems, 14(1), 1-20.
162. Power, M. (2013). The audit society: Rituals of verification (2nd ed.). Oxford University Press.
163. Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2012). Fraud Examination (4th ed.). Cengage Learning.
164. Dorminey, J., Fleming, A. S., Kranacher, M.-J., & Riley, R. A. (2012). The evolution of fraud theory. Issues in Accounting Education, 27(2), 555-579.
165. Reginato, E., Nonnis, C., & Pavan, A. (2012). Modern public internal control systems and accountability in health care organisations. Economia Aziendale Online, 3(2), 149-160.
166. Zhang, C., Pawlicki, A., McReynolds, D., & Titera, W. (2012). A continuous auditing web services model for XML-based accounting systems. International Journal of Accounting Information Systems, 13(2), 55-79.
167. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602-613.
168. Binder, C. (2011). Medicare program integrity: Activities to protect Medicare from payment errors, fraud, and abuse. Congressional Research Service Report R41526.
169. Kranacher, M.-J., Riley, R. A., & Wells, J. T. (2011). Forensic Accounting and Fraud Examination. Wiley.
170. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559-569.
171. Perols, J. L., & Lougee, B. A. (2011). The relation between earnings management and financial statement fraud. Advances in Accounting, 27(1), 39-53.
172. Wells, J. T. (2011). Corporate Fraud Handbook: Prevention and Detection (3rd ed.). Wiley.
173. Zhou, W., & Kapoor, G. (2011). Detecting evolutionary financial statement fraud. Decision Support Systems, 50(3), 570-575.
174. Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2010). Audit Automation: Principles and Problems as Precursors to Continuous Auditing. Working Paper, Rutgers University.

175. Debreceny, R. S., & Gray, G. L. (2010). Data Mining Journal Entries for Fraud Detection: An Exploratory Study. International Journal of Accounting Information Systems, 11(3), 157–181.
176. Dilla, W. N., & Janvrin, D. J. (2010). Where do Experts Look?: An Eye-tracking Investigation of the Search Processes of the Audit of Estimates. Journal of Information Systems, 24(2), 25-48.
177. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A Comprehensive Survey of Data Mining Based Fraud Detection Research. arXiv preprint arXiv:1009.6119.
178. Teeter, R. A. (2010). The Remote Audit. Journal of Emerging Technologies in Accounting, 7(1), 73–88.
179. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1-58.
180. Coderre, D. (2009). Computer-Aided Fraud Prevention and Detection: A Step-by-Step Guide. Wiley.
181. Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2008). Putting continuous auditing theory into practice: Lessons from two pilot implementations. Journal of Information Systems, 22(2), 195-214.
182. Curtis, M. B., & Payne, E. A. (2008). An examination of contextual factors and individual characteristics affecting technology implementation decisions in auditing. International Journal of Accounting Information Systems, 9(2), 104-121.
183. Sparrow, M. K. (2008). Fraud in the U.S. health-care system: Exposing the vulnerabilities of automated payments systems. Social Research, 75(4), 1151-1180.
184. Dowling, C., & Leech, S. (2007). Audit support systems and decision support. International Journal of Accounting Information Systems, 8(2), 92-116.
185. Hunton, J. E., & Rose, J. M. (2004). Effects of PCAOB staff accounting bulletins on auditor judgments. Auditing: A Journal of Practice & Theory, 23(1), 1-19.
186. Braun, R. L., & Davis, H. E. (2003). Computer-assisted audit tools and techniques: Analysis and perspectives. Managerial Auditing Journal, 18(9), 725-731.
187. Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2002). Feasibility and economics of continuous assurance. Auditing: A Journal of Practice & Theory, 21(1), 125-138.
188. Ashcroft, P. (2002). Application of digital analysis in the audit. Today's CPA, 32(4), 26-30.
189. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235–255.
190. Rezaee, Z., Sharbatoghlie, A., Elam, R., & McMickle, P. L. (2002). Continuous auditing: Building automated auditing capability. Auditing: A Journal of Practice & Theory, 21(1), 147–163.
191. Bierstaker, J. L., Burnaby, P., & Thibodeau, J. (2001). The impact of information technology on the audit process. Managerial Auditing Journal, 16(3), 152–158.

192. Nigrini, M. J. (2000). Digital Analysis Using Benford's Law: Tests and Statistics for Auditors. Global Audit Publications.
193. Semi, J. (2024). Purchase-to-pay process performance measurement and automation development by utilizing process mining. LUT University.
194. Donley, G. (2018). The broken Medicare appeals system: Regulatory failure and the potential of federal litigation. Health Matrix, 28, 107–146.
195. Einkamerer, T. F., & Maqbool, J. (2017). Accounts payable: Enhancing the process for efficiency. Applied Management Review, 2(1), 45-58.
196. Ali, N. (2016). E-Invoicing adaptation: Advantages, challenges and strategies to address challenges. Helsinki Metropolia University of Applied Sciences.
197. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). Why should I trust you? Understanding the predictions of any classifier. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1135–1144.
198. van der Aalst, W. M. P. (2016). Process Mining: Data Science in Action (2nd ed.). Springer.
199. Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big data in accounting: An overview. Accounting Horizons, 29(2), 381-396.
200. Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M., & Bouchachia, A. (2014). A survey on concept drift adaptation. ACM Computing Surveys, 46(4), 1-37.