World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Reducing repeat findings and control failures in operationally intensive U.S. enterprises: A data-driven internal audit framework for remediation, loss prevention, and governance improvement

Evans Chingezi [1,*], Last Chingezi [2], Lucy Ganyani [3], Pascal Gbang Yelduora [4] and Munashe Naphtali Mupa [5]

[1] *American University,*
[2] *University of Northern Iowa.*
[3] *Babson College.*
[4] *Park University,*
[5] *Hult International Business School.*
Evans Chingezi; ORCiD: 0009-0006-8524-4355
Last Chingezi; ORCiD: 0009-0008-7787-0094
Lucy Ganyani, ORCiD: 0009-0007-4525-3393
Pascal Gbang Yelduora, ORCiD: 0009-0007-7010-2175
Munashe Naphtali Mupa, ORCiD: 0000-0003-3509-861X

World Journal of Advanced Research and Reviews, 2026, 30(03), 2188-2199

Publication history: Received on 22 May 2026; revised on 27 June 2026; accepted on 29 June 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.30.3.1792

Abstract

Operationally intensive enterprises are especially vulnerable to repeat audit findings because they combine high transaction volumes, distributed assets, complex workflows, decentralized execution, and uneven managerial follow-through. This study develops a data-driven internal audit framework for reducing recurring control failures, preventing avoidable loss, and strengthening governance in such settings. The paper combines a structured review of internal-audit, remediation, fraud, and audit-analytics literature with descriptive analysis of the public Audit Data corpus originally documented by the UCI Machine Learning Repository and widely mirrored on Kaggle. The dataset contains 777 observations across 14 sectors and was designed to support the prediction of suspicious firms using present and historical risk factors. Descriptive analysis of the documented sector counts shows that the three largest sectors account for 52.6% of observations and the top five account for 73.1%, indicating material concentration of auditable exposure. The concentration profile (HHI = 1,406.0; Gini = 0.521) suggests that repeat findings are likely to cluster in large, operationally dense environments while smaller sectors remain susceptible to under-audited tail risk. Based on those patterns and the broader literature, the study proposes a five-stage framework that integrates risk-based planning, root-cause analysis, remediation ownership, analytics-supported exception monitoring, and board-level action tracking. The core argument is that organizations do not reduce repeat findings simply by issuing more audit reports; they reduce them by shortening detection lag, assigning accountable owners, validating corrective action, and continuously measuring whether the same failure mode reappears. The paper contributes a practical governance model for U.S. enterprises seeking to move internal audit from retrospective reporting to a closed-loop assurance and remediation system.

Keywords: Internal Audit; Repeat Findings; Control Failures; Remediation; Continuous Auditing; Audit Analytics; Governance; Loss Prevention; Risk-Based Audit Planning; Operational Controls

* Corresponding author: Evans Chingezi

1. Introduction

Repeat audit findings are one of the clearest warning signals that a control environment is not learning fast enough. A repeated issue usually means that an organization has already paid three times for the same problem: first when the control failed, second when assurance resources were used to identify it, and third when management either implemented a weak corrective action or allowed the issue to recur. In operationally intensive enterprises - including manufacturing, logistics, healthcare delivery, distribution, utilities, construction, agribusiness, and large multi-site service organizations - this cycle is especially costly because control failures propagate through volume, geography, and process interdependence. Inventory errors affect working capital; access-control failures affect fraud exposure; procurement exceptions distort margin; and unresolved operational exceptions migrate into reporting, compliance, and reputational risk.

The contemporary governance environment makes recurrence increasingly difficult to justify. The PCAOB stresses that internal control over financial reporting is a process intended to provide reasonable assurance over reliable financial reporting, while the 2024 Global Internal Audit Standards place explicit emphasis on effective engagement planning, communication of results, and monitoring of management action plans (PCAOB, n.d.; The Institute of Internal Auditors, 2024). COSO likewise treats monitoring as a core component of internal control, not an optional afterthought (COSO, 2013). In practical terms, these standards imply that a finding is not truly "closed" when management records an action point; it is closed only when the underlying failure mechanism has been corrected and subsequent monitoring confirms that the exception pattern has materially changed.

The urgency of this issue is amplified by fraud and loss evidence. The Association of Certified Fraud Examiners' 2024 global study reviewed 1,921 real occupational fraud cases from 138 countries and territories, underscoring the continuing scale of economic damage associated with weak control environments (ACFE, 2024). Although not every repeat finding matures into fraud, persistent control weaknesses increase the probability that operational breakdowns, misstatements, or misappropriation will remain undetected long enough to become material (Donelson, Ege and McInnis, 2017). Consequently, repeat findings should be treated not merely as audit-quality irritants, but as lagging indicators of governance underperformance and emerging financial exposure.

This article addresses the problem by developing a data-driven internal audit framework for operationally intensive U.S. enterprises. It does so in two ways. First, it synthesizes research on remediation, internal-control persistence, continuous auditing, visualization, and audit analytics. Second, it uses the public Audit Data corpus - available through the UCI Machine Learning Repository and mirrored on Kaggle - as an empirical illustration of how auditable exposure clusters across sectors and how a more disciplined remediation architecture can be built from documented risk-factor structures (Hooda, 2018; Kaggle, n.d.). The central proposition is straightforward: organizations reduce repeat findings when audit planning is tied to recurrence signals, corrective action is grounded in root-cause evidence, and management follow-through is tracked with continuous exception analytics rather than annual narrative updates.

2. Literature Review

2.1. Repeat findings, persistence, and the economics of weak remediation

Research on internal control persistence shows that repeated weaknesses are not random events; they are usually symptoms of deeper structural problems. Gordon and Wilford (2012) show that multiple consecutive years of material weaknesses represent a distinctive persistence problem rather than a simple continuation of isolated deficiencies. Goh (2009) further demonstrates that governance quality matters for remediation: stronger audit committees and boards are associated with more effective correction of material weaknesses. Graham and Bedard (2013) reinforce the point by showing that remediation outcomes are shaped by the quality of both client processes and auditor interaction under Section 404 environments. Together, these studies suggest that repeat findings arise not only from deficient controls, but also from governance arrangements that fail to convert audit information into sustained operational change.

From a management perspective, the cost of recurrence is cumulative. An unresolved exception consumes staff time in each reporting cycle; forces repeat testing by internal and external assurance providers and weakens confidence in management's control narrative. In operational settings with thousands of transactions or large physical asset footprints, persistence also magnifies loss exposure because the same control gap remains available for re-exploitation. Repeat findings therefore signal a breakdown in institutional learning: the organization sees the problem, documents the problem, and discusses the problem, but does not re-engineer the process conditions that produced it.

2.2. Human capability, ownership, and root-cause discipline

Persistent weaknesses are frequently associated with deficits in control ownership, segregation of duties, and control-capable staffing. Choi et al. (2013) show that investment in internal-control human resources is materially relevant to disclosed control weakness outcomes, indicating that remediation capacity depends in part on whether organizations allocate sufficiently skilled personnel to control design, operation, and follow-up. This matters in operationally intensive enterprises where many control breakdowns occur at the interface between finance and operations: stock receipt, maintenance authorization, work-order approval, supplier onboarding, access provisioning, project certification, or field-level revenue recognition.

The implication is that effective remediation cannot be reduced to generic action plans such as "retrain staff" or "increase supervision." Root-cause analysis must distinguish among design failure, execution failure, systems failure, data-quality failure, accountability failure, and governance failure. Without that distinction, remediation activity often addresses the visible symptom rather than the causal architecture. A repeated reconciliation problem, for example, may not be a reconciliation problem at all; it may be a master-data governance problem or a workflow sequencing problem upstream of the close process.

2.3. Continuous auditing and analytics-supported exception review

The literature on continuous auditing offers a direct response to the recurrence problem. Joshi and Marthandan (2020) argue that big-data techniques can materially enhance continuous internal auditing by expanding the coverage, speed, and pattern-detection capacity of assurance work. Eulerich, Georgi and Schmidt (2020) similarly position risk-based planning and continuous auditing as mutually reinforcing: continuous signals improve the quality of annual planning, while risk-based planning helps focus continuous procedures on the most consequential auditable areas. In other words, the annual audit plan should not be isolated from live control data; it should be updated by it.

Recent research also emphasizes that analytics are most effective when they remain interpretable and decision useful. Baaske, Eulerich and Wood (2025) show that data-analytic visualizations can improve anomaly identification, particularly when users receive feedback that helps them translate visual patterns into audit judgments. Wang, Ferreira and Yan (2025) extend the planning literature by proposing an integrated, multi-stage approach that links risk assessment, audit selection, and resource allocation. These findings matter because repeat findings are often allowed to persist simply because organizations do not convert dispersed exception evidence into prioritized, visible, and actionable remediation agendas.

2.4. AI, anomaly detection, and modern audit planning

The audit profession's movement toward artificial intelligence and advanced analytics strengthens the case for continuous remediation monitoring. Fedyk et al. (2022) show that AI adoption is becoming a measurable feature of the audit process rather than a speculative future development. The value of AI in this context is not merely automation for its own sake; it is the ability to detect subtle, repeated, or low-frequency patterns that traditional periodic reviews can miss. For repeat findings, that means shorter detection lag, broader population coverage, and better prioritization of exceptions requiring escalation.

This direction is also reflected in emerging work connected to the user's research profile. Netshifhefhe et al. (2024a) argue that internal auditing and legal compliance become more effective when treated as integrated rather than siloed governance functions. Netshifhefhe et al. (2024b) further position forensic auditing as a governance-strengthening mechanism in environments with elevated fraud and compliance risk. Homwe et al. (2025) show how interpretable machine learning can improve audit planning in financial services, while Taanisa et al. (2026) propose AI-enabled audit analytics for anomaly detection and control strengthening. Read together, these studies support a practical shift: internal audit should not focus solely on whether controls failed; it should also maintain a data-enabled early-warning architecture that identifies where recurrence risk is building.

3. Materials and Methods

This study adopts a descriptive-analytical design. It does not claim to estimate a universal causal model of repeat findings across all industries. Instead, it uses a public audit-risk corpus to illustrate how a documented dataset structure can support more disciplined audit planning and remediation governance and then integrates those empirical signals with internal-audit and control-remediation literature to develop an enterprise-ready framework for U.S. operational settings.

The empirical source is the Audit Data dataset created by Hooda (2018) and hosted in the UCI Machine Learning Repository, with a widely used mirror available on Kaggle. According to the official UCI documentation, the dataset contains 777 observations drawn from one year of non-confidential records from the Auditor Office of India for 2015-2016 and was designed to support the classification of suspicious firms using present and historical risk factors (Hooda, 2018). UCI further documents the sector composition and explains that the risk factors were derived from sources including past audit records, audit-paras, environmental condition reports, firm reputation summaries, ongoing issues reports, profit-value records, loss-value records, and follow-up reports (Hooda, 2018). The Kaggle mirror preserves the dataset's utility for practitioners and researchers seeking a readily accessible audit-risk corpus for experimentation and teaching (Kaggle, n.d.).

Because the public documentation available for this study provides complete sector counts and variable-family descriptions, but not a fully reproducible in-container row-level extract for direct re-estimation, the quantitative component focuses on documented distributions and concentration analysis. The following metrics were computed from the documented sector counts:

(i) sector shares and cumulative shares;
(ii) concentration ratios for the top three and top five sectors;
(iii) the Herfindahl-Hirschman Index (HHI) as a measure of concentration; and
(iv) the Gini coefficient and Shannon evenness as descriptive indicators of exposure balance.

The analytical logic is as follows. If auditable exposure is concentrated, then recurrence management should allocate disproportional follow-up effort to the largest and most operationally dense environments while still protecting against tail-risk neglect in smaller units. If the documented variable families span both historical and current risk signals, then repeat findings should be managed through a closed-loop system that combines past-failure memory, current exception detection, and follow-up validation. On that basis, the study develops a five-stage internal audit framework and a remediation priority matrix for use in operationally intensive U.S. enterprises.

A limitation should be stated clearly. The public audit-risk dataset is not a U.S.-only dataset; it originates from the Auditor Office of India. However, the control mechanisms represented in the data - historical findings, exception reporting, follow-up records, and operational risk signals - are structurally relevant to U.S. enterprises operating under COSO, PCAOB, and IIA governance expectations. The value of the dataset in this paper is therefore not jurisdictional identity, but its usefulness as a public audit-risk corpus from which recurrence-sensitive audit design principles can be derived.

Table 1 Profile of the public Audit Data corpus used for empirical illustration

Characteristic	**Value**
Source dataset	Audit Data
Primary source	UCI Machine Learning Repository
Kaggle access	Public Kaggle mirror of the Audit Data corpus
Creator	Nishtha Hooda
Observation period	2015-2016
Observations	777
Sectors documented	14
Primary research objective	Classification of suspicious firms using present and historical risk factors
Documented variable families	Past audit records; audit-paras; environmental reports; firm reputation; ongoing issues; profit-value records; loss-value records; follow-up reports

Source: compiled from Hooda (2018) and Kaggle (n.d.).

4. Results

4.1. Sector concentration and auditable exposure

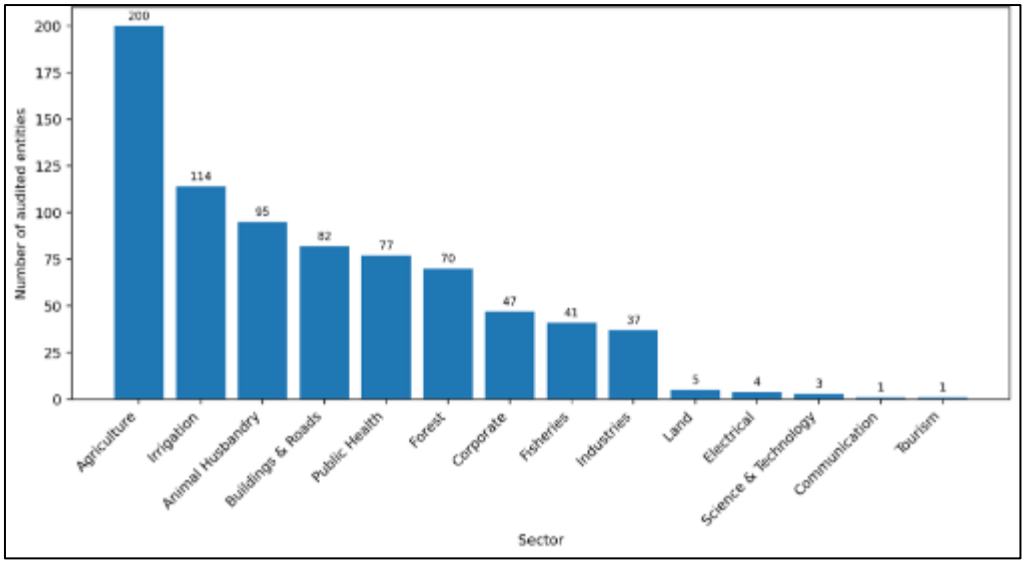
The documented sector counts reveal a materially uneven distribution of auditable exposure. Agriculture alone accounts for 25.74% of observations, followed by Irrigation at 14.67% and Animal Husbandry at 12.23%. Together, these three sectors represent 52.64% of the full dataset. When Buildings and Roads (10.55%) and Public Health (9.91%) are added, the top five sectors account for 73.10% of all observations. Figure 1 and Figure 3 show that the population is not evenly distributed across auditable environments; rather, it is dominated by a relatively small number of high-volume sectors.

The concentration measures confirm that interpretation. The HHI of 1406.0 indicates a moderate concentration profile rather than an atomized risk universe, while the Gini coefficient of 0.521 signals meaningful inequality in exposure across sectors. At the same time, Shannon evenness of 0.811 indicates that the dataset is not completely dominated by a single sector. This is an important governance insight. Repeat findings in large sectors deserve intensified remediation because they drive most of the auditable exposure, but smaller sectors should not be ignored simply because they contribute less volume. Tail-risk environments often escape sustained monitoring precisely because they appear numerically insignificant in annual plans.

Table 2 Documented sector distribution of the Audit Data corpus

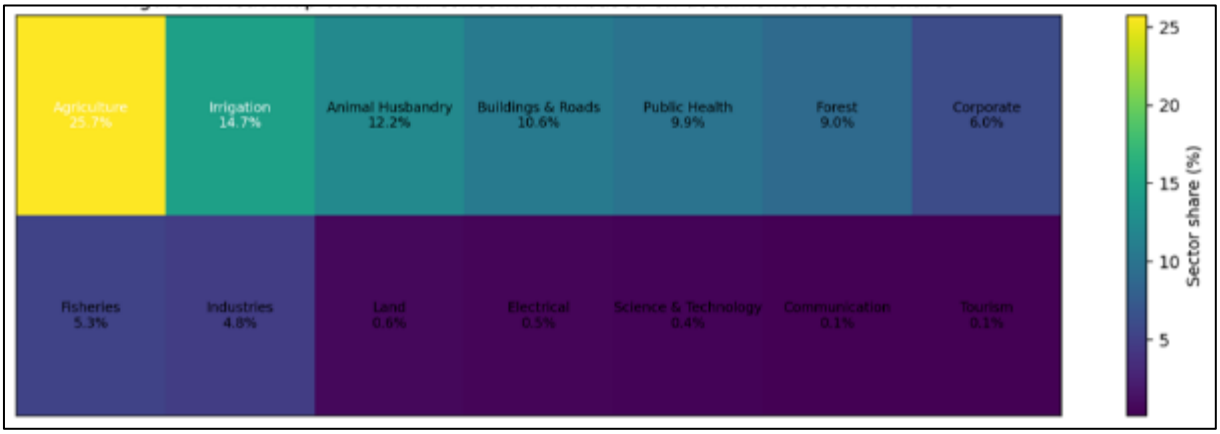
Sector	Count	Share (%)	Cumulative share (%)
Agriculture	200	25.74	25.74
Irrigation	114	14.67	40.41
Animal Husbandry	95	12.23	52.64
Buildings & Roads	82	10.55	63.19
Public Health	77	9.91	73.10
Forest	70	9.01	82.11
Corporate	47	6.05	88.16
Fisheries	41	5.28	93.44
Industries	37	4.76	98.20
Land	5	0.64	98.84
Electrical	4	0.51	99.36
Science & Technology	3	0.39	99.74
Communication	1	0.13	99.87
Tourism	1	0.13	100.00

Source: computed from sector counts documented by Hooda (2018).



Source: author's computation from Hooda (2018).

Figure 1 Sector distribution in the public Audit Data corpus (N = 777)



Source: author's computation from Hooda (2018).

Figure 2 Heat map of sectoral concentration based on documented sector shares

The heat map of sector shares in Figure 2 makes the practical point visually clear. The risk universe has a thick operational core and a thin peripheral tail. A mature internal audit function should therefore avoid two opposite errors: over-spreading scarce assurance resources uniformly across all units and over-concentrating them in high-volume units without protecting against severe but less frequent exceptions elsewhere. Risk-based planning is strongest when it combines weighted concentration with escalation rules for severity and recurrence.

The variable architecture documented by UCI is equally informative. Because the dataset draws from past audit records, audit-paras, environmental reports, reputation summaries, ongoing issues reports, profit and loss value records, and follow-up reports, it captures precisely the kinds of signals that should inform repeat-finding prevention. Historical findings show whether a control issue has memory. Ongoing-issues reports show whether management has unresolved execution problems. Follow-up reports show whether closure is substantive or merely administrative. Profit/loss and environmental indicators help auditors distinguish routine control exceptions from those arising in stressed operational conditions. In combination, these features point to a governance lesson: recurrence risk is rarely a single-data-point problem. It is a pattern-recognition problem that must be monitored across time and across control domains.

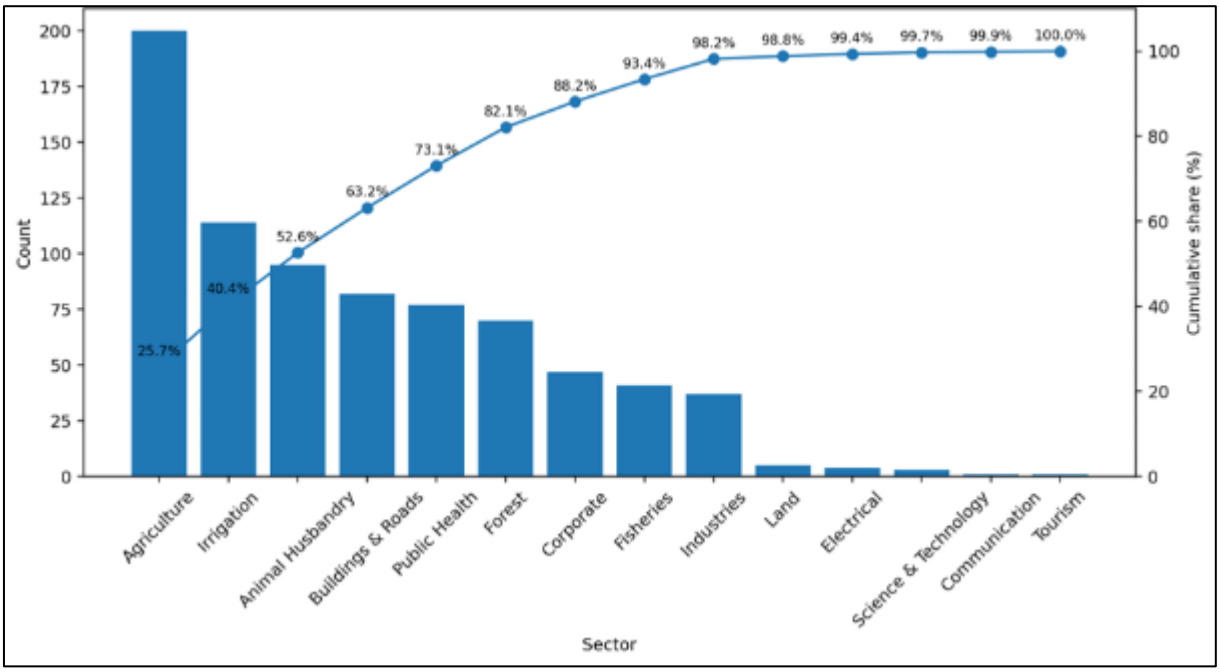
The empirical implication for U.S. enterprises is that remediation governance should be built around patterns, not one-off findings. A stock-adjustment exception should immediately be linked to prior inventory findings, to the speed and quality of prior corrective action, to the materiality of recent write-offs, and to whether related access-control or segregation-of-duties issues remain open. A procurement override should likewise be linked to vendor-master

governance, approval workflows, and previous contract-compliance findings. The point is not merely to classify findings; it is to connect them into recurring failure chains.

Table 3 Concentration metrics derived from documented sector counts

Metric	Value	Interpretive implication
Top 3 sector share	52.64%	More than half of documented exposure sits in the three largest sectors; repeat-finding surveillance should be weighted accordingly.
Top 5 sector share	73.10%	Audit resources concentrated only on small units would miss most auditable exposure.
HHI	1406.0	Moderate concentration: exposure is neither fully dispersed nor monopolized by one sector.
Gini coefficient	0.521	Meaningful inequality in sector exposure; some sectors are structurally more important to the audit universe.
Shannon evenness	0.811	Despite concentration, exposure remains broad enough to require portfolio-style planning rather than single-sector focus.

Source: author's computation from Hooda (2018).



Source: author's computation from Hooda (2018).

Figure 3 Pareto profile of auditable exposure across sectors

4.2. Risk architecture and repeat-finding relevance

Table 4 translates the documented data families in the public corpus into a recurrence-management logic suitable for internal audit. The purpose is not to force the dataset into a narrow fraud-only interpretation, but to show how historical, contextual, financial, and follow-up signals can be operationalized in a repeat-finding prevention model.

Table 4 Mapping documented data families to repeat-finding prevention logic

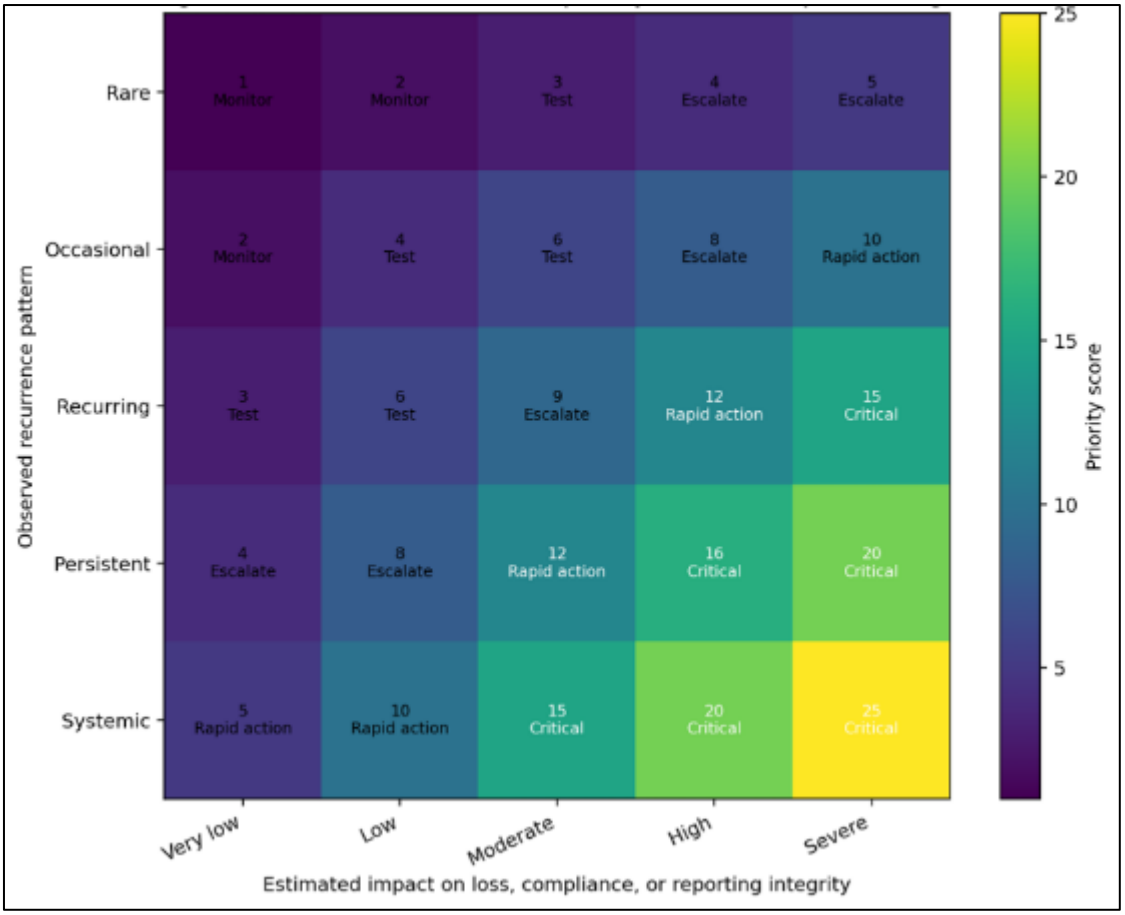
Documented data family	Control relevance	Why it matters for repeat findings	Audit response implication
Past audit records	Historical memory of failure	Identifies whether the same issue or control theme has appeared before	Use as a recurrence flag in annual planning and issue escalation
Audit-paras	Documented exceptions and observations	Shows the severity and nature of prior deficiencies	Prioritize testing where prior paras remain unresolved or repeatedly reappear
Environmental condition reports	Operating context and stress factors	Helps explain why failures occur under certain field or operational conditions	Adjust control testing for context-specific risks such as dispersed operations or unstable processes
Firm reputation summaries	Tone, discipline, and governance signal	Persistent integrity concerns often coexist with recurring control issues	Integrate governance and compliance indicators into audit prioritization
Ongoing issues reports	Current unresolved execution problems	Open issues are leading indicators of future repeat findings	Track unresolved items continuously rather than annually
Profit/loss value records	Financial pressure and consequence profile	High pressure or high-value variance environments can intensify override incentives	Escalate remediation in areas with both control weakness and material value impact
Follow-up reports	Management adoption and closure quality	Shows whether prior corrective action changed behaviour or simply closed paperwork	Validate closure with evidence and post-remediation testing

Source: adapted from the documented variable families in Hooda (2018), interpreted through the internal-audit literature.

5. A Data-Driven Internal Audit Framework for Reducing Repeat Findings

The framework proposed in this study rests on five integrated stages. The first is recurrence-sensitive risk sensing. Annual planning should incorporate not only inherent and control risk, but also recurrence indicators such as the age of open findings, the frequency of repeat exceptions, the number of prior failed remediation attempts, and the lag between issue detection and formal escalation. This extends traditional risk-based planning in a way consistent with continuous auditing and integrated planning literature (Eulerich, Georgi and Schmidt, 2020; Wang, Ferreira and Yan, 2025).

The second stage is root-cause qualification. Audit teams should code each significant finding against a standard taxonomy - design deficiency, execution failure, systems configuration, master-data weakness, oversight failure, policy ambiguity, competence gap, or accountability failure. Without such a taxonomy, organizations tend to close findings administratively rather than causally. The evidence from governance and remediation studies suggests that causal clarity is a precondition for durable remediation (Goh, 2009; Graham and Bedard, 2013; Choi et al., 2013).



Source: framework developed in this study from recurrence, severity, and remediation governance principles.

Figure 4 Data-driven remediation priority matrix for repeat findings

The third stage is accountable remediation design. Every material finding should carry a named business owner, deadline, validation method, and evidence requirement. Action plans should specify how the control environment will behave differently after remediation, not merely which meeting was held or which memo was circulated. Where the issue intersects with regulatory obligations, legal and compliance functions should be directly integrated into action design, consistent with the integrated governance logic advanced by Netshifhefhe et al. (2024a).

The fourth stage is analytics-supported exception monitoring. Instead of waiting for the next audit cycle, internal audit should implement rule-based or model-assisted monitoring over the relevant transaction or process population. In an inventory environment, that may include negative stock events, abnormal adjustments, override frequency, unmatched goods receipts, or late cycle counts. In a procurement environment, it may include duplicate vendors, threshold splitting, purchase-order bypass, or unauthorized rate changes. In a project or service-delivery environment, it may include back-dated approvals, unmatched completion certificates, or unusual manual journal entries. This is where continuous auditing, visualization, and interpretable analytics create operational value (Joshi and Marthandan, 2020; Baaske, Eulerich and Wood, 2025; Homwe et al., 2025; Taanisa et al., 2026).

The fifth stage is governance escalation and closure validation. The board, audit committee, or equivalent oversight body should receive periodic reporting not just on open findings, but on recurrence indicators: repeat-finding rate, closure cycle time, overdue action-point ratio, percentage of findings re-opened after claimed closure, and financial leakage attributable to recurring failures. In effect, the governance question should shift from “How many findings remain open?” to “How many failure mechanisms are still alive?” That shift aligns with the monitoring emphasis embedded in COSO and the Global Internal Audit Standards (COSO, 2013; The Institute of Internal Auditors, 2024).

For U.S. operationally intensive enterprises, this framework has three practical implications. First, internal audit should be embedded more deeply in operational data streams so that audit planning reflects current exception patterns rather than only prior-year risk assessments. Second, remediation should be treated as an operational redesign exercise, not a paperwork exercise. Third, governance reporting should explicitly distinguish between new findings and recurring

findings, because the latter are stronger indicators of structural weakness. Organizations that make that distinction will allocate corrective effort more efficiently and improve both control reliability and credibility with external stakeholders.

Table 5 Five-stage framework for remediation, loss prevention, and governance improvement

Framework stage	Core question	Primary data inputs	Typical owner	Illustrative KPI
1. Recurrence-sensitive risk sensing	Where is repeat failure most likely to reappear?	Prior findings, exception logs, open action points, process volumes, risk indicators	Chief audit executive / audit manager	Repeat-finding rate
2. Root-cause qualification	Why did the control fail?	Workpapers, process maps, walkthroughs, interviews, system logs	Audit lead with business process owner	Percentage of findings coded to validated root cause
3. Accountable remediation design	What must change and who will own it?	Action plans, policy updates, system-change requests, training records	Business owner with risk/compliance support	Overdue action-point ratio
4. Continuous exception monitoring	Has the failure pattern materially changed?	ERP data, exception dashboards, alerts, reconciliation outputs, user-access logs	Internal audit analytics / control owner	Exception detection lag
5. Governance validation and closure	Can the issue be credibly closed?	Validation testing, evidence packs, committee reporting, re-performance results	Audit committee / executive risk forum	Re-opened findings as % of closed findings

Source: developed in this study from the literature and the documented structure of the Audit Data corpus.

6. Discussion and Implications for U.S. Enterprises

Although the public dataset used for illustration originates outside the United States, its structural lessons travel well to U.S. operational settings. Enterprises with distributed assets, field operations, regulated transactions, procurement complexity, and high exception volumes face the same central question: can they translate audit knowledge into faster, better, and more durable control correction? The framework proposed here answers that question by shifting the center of gravity from annual reporting to continuous governance learning.

For chief audit executives, the most immediate implication is methodological: recurrence indicators should become explicit planning variables. For management teams, the implication is operational: remediation must be designed as a process-change intervention with measurable evidence of behavioural change. For boards and audit committees, the implication is oversight-focused: closure quality and recurrence trends should receive more attention than raw open-item counts.

6.1. Implications for Internal Audit Practice

The findings of this study suggest that internal audit functions should place greater emphasis on recurrence prevention rather than simply identifying control deficiencies. Consistent with prior research, repeat findings often indicate underlying weaknesses in remediation, accountability, or governance rather than isolated control failures (Gordon & Wilford, 2012; Goh, 2009). As a result, internal auditors should incorporate recurrence indicators, unresolved action plans, and historical findings into risk-based planning and follow-up activities.

The proposed five-stage framework highlights the importance of combining root-cause analysis, accountable remediation, and continuous exception monitoring to reduce the likelihood of recurring control failures. Rather than treating findings as closed when corrective actions are reported, internal auditors should validate whether remediation has changed underlying processes and prevented reoccurrence (Graham & Bedard, 2013). This approach aligns with the monitoring principles of COSO (2013) and the Global Internal Audit Standards (IIA, 2024), which emphasize ongoing evaluation of control effectiveness and management action plans.

The study further demonstrates that analytics-supported monitoring can strengthen internal audit effectiveness by identifying recurrence patterns, unresolved issues, and emerging control risks earlier in the remediation cycle. By integrating recurrence-sensitive planning with continuous monitoring and governance oversight, internal audit functions can improve loss prevention, strengthen accountability, and contribute more effectively to organizational resilience and long-term governance performance (Joshi & Marthandan, 2020; Eulerich, Georgi & Schmidt, 2020).

7. Conclusion

This study set out to answer a practical governance question: how can operationally intensive U.S. enterprises reduce repeat findings and control failures in a way that materially improves loss prevention and governance performance? The answer developed here is that recurrence falls when internal audit becomes a closed-loop system rather than a periodic reporting function. Using documented evidence from the public Audit Data corpus, the paper showed that auditable exposure is concentrated and that recurrence-sensitive planning should therefore focus disproportionate attention on the largest and most operationally complex environments while still guarding against neglected tail risk. Drawing on internal-control, remediation, and audit-analytics literature, the paper then developed a five-stage framework combining risk-based planning, root-cause analysis, accountable remediation, continuous exception monitoring, and oversight-level validation.

The broader implication is that repeat findings are not simply audit outcomes; they are governance diagnostics. Where the same weakness returns, management has not yet converted assurance information into durable operational change. A modern internal audit function should therefore measure success not by the number of reports issued, but by the speed with which organizations detect failure, correct root causes, and prevent reappearance. That is the foundation of a stronger control environment, lower avoidable loss, and more credible governance.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Association of Certified Fraud Examiners (ACFE) (2024) Occupational Fraud 2024: A Report to the Nations. Austin, TX: ACFE.

[2] Baaske, B.N., Eulerich, M. and Wood, D.A. (2025) 'Improving Audit Quality with Data Analytic Visualizations: The Importance of Spatial Abilities and Feedback in Anomaly Identification', Accounting Horizons, 39(3), pp. 85-97. doi: 10.2308/HORIZONS-2023-073.

[3] Choi, J.-H., Choi, S., Hogan, C.E. and Lee, J. (2013) 'The Effect of Human Resource Investment in Internal Control on the Disclosure of Internal Control Weaknesses', Auditing: A Journal of Practice & Theory, 32(4), pp. 169-199.

[4] Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013) Internal Control - Integrated Framework: Executive Summary. New York: COSO.

[5] Donelson, D.C., Ege, M.S. and McInnis, J.M. (2017) 'Internal Control Weaknesses and Financial Reporting Fraud', Auditing: A Journal of Practice & Theory, 36(3), pp. 45-69. doi: 10.2308/ajpt-51608.

[6] Eulerich, M., Georgi, C. and Schmidt, A. (2020) 'Continuous Auditing and Risk-Based Audit Planning - An Empirical Analysis', Journal of Emerging Technologies in Accounting, 17(2).

[7] Fedyk, A., Hodson, J., Khimich, N. and Fedyk, T. (2022) 'Is artificial intelligence improving the audit process?', Review of Accounting Studies, 27, pp. 938-985. doi: 10.1007/s11142-022-09697-x.

[8] Goh, B.W. (2009) 'Audit Committees, Boards of Directors, and Remediation of Material Weaknesses in Internal Control', Contemporary Accounting Research, 26(2), pp. 549-579. doi: 10.1506/CAR.26.2.9.

[9] Gordon, L.A. and Wilford, A.L. (2012) 'An Analysis of Multiple Consecutive Years of Material Weaknesses in Internal Control', The Accounting Review, 87(6), pp. 2027-2060. doi: 10.2308/accr-50211.

[10] Graham, L. and Bedard, J.C. (2013) 'The Influence of Auditor and Client Section 404 Processes on Remediation of Internal Control Deficiencies at All Levels of Severity', Auditing: A Journal of Practice & Theory, 32(4), pp. 45-69. doi: 10.2308/ajpt-10355.

[11] Hooda, N. (2018) Audit Data [Dataset]. UCI Machine Learning Repository. doi: 10.24432/C5930Q.

[12] Homwe, T., Mupa, M.N., Matope, A., Mlambo, N., Chingezi, L. and Chihota, T.A. (2025) 'Interpretable machine learning for audit planning: Improving misstatement and compliance risk detection in financial services', World Journal of Advanced Research and Reviews, 28(2), pp. 925-933. doi: 10.30574/wjarr.2025.28.2.3779.

[13] Kaggle (n.d.) Audit Data. Available at: https://www.kaggle.com/datasets/sid321axn/audit-data (Accessed: 20 June 2026).

[14] Netshifhefhe, K., Netshifhefhe, M.V., Mupa, M.N. and Murapa, K.A. (2024a) 'Integrating Internal Auditing and Legal Compliance: A Strategic Approach to Risk Management', Iconic Research and Engineering Journals, 8(4), pp. 446-465.

[15] Netshifhefhe, K., Netshifhefhe, M.V., Mupa, M.N. and Murapa, K.A. (2024b) 'The Role of Forensic Audits in Strengthening Corporate Governance and Mitigating Compliance Risks', Iconic Research and Engineering Journals, 8(4), pp. 427-445.

[16] Public Company Accounting Oversight Board (PCAOB) (n.d.) AS 2201: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements. Available at: https://pcaobus.org/oversight/standards/auditing-standards/details/AS2201 (Accessed: 20 June 2026).

[17] Taanisa, T., Mukwata, N.A., Sydney, J., Ganyani, L., Maturure, R.N., Chingezi, E., Yelduora, P.G. and Mupa, M.N. (2026) 'AI-Enabled Audit Analytics for SME Financial Reporting and Anomaly Detection: A Risk-Based Framework for Early Irregularity Identification and Control Strengthening', World Journal of Advanced Research and Reviews, 30(3), pp. 1113-1126. doi: 10.30574/wjarr.2026.30.3.1596.

[18] The Institute of Internal Auditors (2024) Global Internal Audit Standards. Lake Mary, FL: The Institute of Internal Auditors.

[19] Wang, X., Ferreira, F.A.F. and Yan, P. (2025) 'A multi-objective optimization approach for integrated risk-based internal audit planning', Annals of Operations Research, 346(2), pp. 1811-1840. doi: 10.1007/s10479-023-05228-2.

[20] Joshi, P.L. and Marthandan, G. (2020) 'Continuous internal auditing: can big data analytics help?', International Journal of Accounting, Auditing and Performance Evaluation, 16(1), pp. 25-42. doi: 10.1504/IJAAPE.2020.106766.

[21] The Institute of Internal Auditors. (2024). Global Internal Audit Standards. The Institute of Internal Auditors.