Enterprise ERP Wrapper Automation for SOX Evidence Extraction

Naga Venkata Ganesh Kumar Puvvula
3518 Prickly Pear Path,
Melissa, TX, 75454, USA

ABSTRACT
In many global Enterprise Resource Planning (ERP) environments, Sarbanes-Oxley (SOX) compliance activities still depend heavily on manual evidence collection, making audit preparation slow, repetitive, and resource-intensive. Finance and compliance teams often spend significant time gathering screenshots, validating transaction histories, and organizing supporting documents for quarterly audits. This paper presents a practical automation framework developed within Oracle E-Business Suite that streamlines SOX evidence extraction through specialized "SOX Automation Wrapper Programs." The framework replaces fragmented screenshot-based processes with a centralized, program-driven extraction model that allows users to retrieve audit evidence directly from the ERP system in a standardized format. By automating evidence generation and reporting, the solution reduced quarterly compliance effort from nearly 40 hours to approximately 1 hour, resulting in a 97.5% improvement in operational efficiency. In addition to improving audit readiness, the framework supports ASC 606 revenue-recognition compliance and offers a scalable approach for enterprises transitioning from legacy Oracle environments to modern cloud ecosystems such as Workday and Zuora.

General Terms
Enterprise Governance, Risk and Compliance; SOX Compliance; ERP Automation; Continuous Auditing; Internal Controls.

Keywords
eGRC, SOX Compliance, Oracle EBS, ERP Automation, ASC 606, Continuous Auditing, IT General Controls (ITGC), Financial Reporting Quality.

1. INTRODUCTION
In today's rapidly evolving digital economy, Enterprise Governance, Risk, and Compliance (eGRC) has become a continuous operational responsibility rather than a periodic audit exercise. Organizations operating in heavily regulated industries are expected to maintain strong Internal Controls over Financial Reporting (ICFR), particularly under the requirements of the Sarbanes-Oxley Act (SOX) Section 404. This requires enterprises not only to establish effective controls, but also to continuously demonstrate and document that those controls are functioning correctly. As a result, compliance activities have become deeply integrated into everyday financial and technology operations.

Despite advances in Enterprise Resource Planning (ERP) systems, many organizations still rely on highly manual methods for compliance evidence gathering. Finance and technology teams often spend significant time extracting transaction data, validating system configurations, collecting screenshots, reviewing user-access records, and compiling supporting documents for auditors. These repetitive activities create operational inefficiencies and increase the likelihood of human error, particularly in large multinational environments where thousands of transactions and configurations must be validated across different business units and systems. Prior research in Information Systems auditing has consistently highlighted that manual evidence collection is both resource-intensive and difficult to scale effectively [1].

Beyond the operational burden, manual compliance processes also create a strategic challenge. Highly skilled financial technology resources are frequently diverted away from innovation and transformation initiatives in order to support recurring audit and compliance requests. This slows modernization efforts and limits the organization's ability to respond to changing regulatory and business demands.

This paper presents the implementation of a high-impact automation framework designed to streamline SOX evidence extraction within Oracle E-Business Suite. The solution introduces specialized "SOX Automation Wrapper Programs" that automate the retrieval, validation, and reporting of control evidence directly from the ERP environment. By replacing fragmented screenshot-based workflows with a standardized, self-service extraction architecture, the framework significantly reduced compliance effort while improving audit consistency and traceability. The study further demonstrates how targeted ERP automation can bridge the gap between legacy Oracle systems and the increasing demands of modern, high-velocity compliance environments.

2. LITERATURE REVIEW
2.1 The Shift Toward Continuous Auditing and Monitoring
The traditional model of auditing has gradually evolved from periodic verification toward continuous monitoring and real-time control validation. In large enterprises, financial transactions occur at a scale and speed that make retrospective sampling increasingly insufficient for identifying operational or compliance risks. As a result, researchers have emphasized the importance of Continuous Auditing (CA), where controls and transactions are evaluated continuously rather than only during scheduled audit cycles [2]. This shift is particularly important in ERP-driven environments, where a single configuration change or approval override can affect thousands of downstream financial transactions before a manual audit identifies the issue.

Traditional audit processes often depend on historical samples, spreadsheets, and manual evidence collection. While this approach may satisfy baseline compliance requirements, it creates a delay between the occurrence of a control issue and its detection. Automated extraction and monitoring systems reduce this "audit lag" by allowing organizations to analyze complete populations of transactional and configuration data in near real time rather than relying on selective samples.

The "SOX Automation Wrapper" framework presented in this study aligns closely with the principles of Continuous Monitoring. Instead of requiring finance or technology teams to manually capture screenshots or validate configurations periodically, the system automatically extracts and validates control evidence directly from Oracle E-Business Suite. Examples include automated verification of journal approval settings, depreciation configurations, user-access assignments, and workflow responsibilities. Recent research also suggests that automation and AI-driven auditing reduce the burden of repetitive compliance tasks, enabling auditors and finance professionals to focus more on risk evaluation, anomaly detection, and strategic analysis rather than administrative evidence gathering [3]. In this sense, automation does not eliminate the role of auditors; it reshapes the nature of their work toward higher-value oversight and governance activities.

2.2 ERP Governance and the Pervasiveness of IT General Controls (ITGCs)

Enterprise Resource Planning (ERP) systems such as Oracle and Workday function as the central operational backbone of modern organizations. Since financial reporting, procurement, payroll, access management, and approval workflows are integrated into these systems, ERP governance has become closely tied to the effectiveness of organizational internal controls. The reliability of financial reporting increasingly depends on the integrity of ERP configurations, user permissions, workflow approvals, and audit trails.

However, despite the sophistication of modern ERP platforms, organizations frequently continue to rely on manual workarounds when preparing compliance evidence or validating controls [4]. These manual interventions introduce inconsistency and weaken the reliability of Internal Controls over Financial Reporting (ICFR). Prior studies have shown that Segregation of Duties (SoD) conflicts and inappropriate access privileges remain among the most common failures within IT General Controls (ITGCs) [5]. Such failures are particularly significant because they affect the foundational integrity of the ERP environment itself rather than isolated business processes.

Research also indicates that automated controls are often viewed more favorably than manual controls by auditors, regulators, and equity markets because they are less vulnerable to fatigue, inconsistency, and management override [6]. Controls embedded directly within ERP systems provide greater repeatability, traceability, and reliability compared to spreadsheet-driven validations. The framework proposed in this paper addresses these concerns by introducing automated "Responsibility by Function" and "User Listing" extracts that continuously validate access structures and functional responsibilities within Oracle E-Business Suite. By automating these pervasive ITGC validations, the framework strengthens the security and auditability of the ERP foundation itself while reducing the operational burden associated with recurring SOX compliance activities.

3. METHODOLOGY: THE SOX AUTOMATION WRAPPER ARCHITECTURE

The primary technical contribution of this study is the development of a multi-modular automation framework within Oracle E-Business Suite (EBS) designed specifically for SOX evidence extraction and compliance reporting. The methodology focused on eliminating the traditional manual workflow commonly followed during audit preparation, where users repeatedly logged into the ERP system, navigated through configuration screens, captured screenshots, exported reports, and manually uploaded evidence for audit review.

This traditional "Login–Capture–Upload" cycle was both time-consuming and operationally inefficient, especially in large enterprise environments where multiple controls had to be validated across finance, payables, receivables, and fixed-asset modules. The proposed framework replaced this fragmented approach with a centralized "Submit–Notify–Review" model in which evidence extraction is executed programmatically through Oracle Concurrent Programs. The architecture was designed not only to automate reporting but also to improve consistency, audit traceability, and security segregation within the ERP environment.

3.1 Module 1: The Master Wrapper Program

At the center of the framework is the Master Wrapper Program, a centralized concurrent-processing layer engineered to consolidate multiple SOX-related extracts into a single execution stream. Instead of requiring users to execute reports individually across different Oracle modules, the wrapper triggers multiple reporting jobs simultaneously and compiles the outputs into a standardized evidence package.

The wrapper automates several high-risk financial and access-control validations. One of its key functions is generating Bank Account Extracts, which provide details such as bank branches, account numbers, and associated cash-management configurations. These extracts support verification of cash-management controls and reduce the need for manual navigation through banking setup screens.

The framework also performs Ledger Validation reporting by identifying central accounting hubs where journal approvals are enabled. This control is important because unauthorized or improperly approved journal postings represent a significant financial-reporting risk. By automatically extracting these configurations, the system creates a consistent audit trail for approval-related controls.

Another major component of the wrapper involves Access Control Tracking. The system extracts enterprise-wide user listings along with function-level responsibilities across Finance, Payables, and Receivables modules. These reports are used to validate Segregation of Duties (SoD) compliance and identify users with potentially conflicting access privileges. By centralizing these extracts into one execution framework, the system significantly reduces the manual effort previously required during quarterly SOX testing cycles.

3.2 Module 2: Fixed Asset (FA) Automation

To address SOX FA.2 compliance requirements, a dedicated Fixed Assets (FA) automation sub-wrapper was developed within the framework. Fixed Asset accounting is considered a high-risk financial-reporting area because incorrect depreciation methods, prorate conventions, or calendar configurations can materially affect financial statements and asset valuation.

The automation module extracts and validates key asset-management configurations directly from Oracle EBS, including Asset Depreciation Methods, Prorate Conventions, and Asset Calendars. These reports provide auditors and finance teams with structured evidence supporting the organization's asset-accounting policies and depreciation calculations.

Before automation, auditors often relied on screenshots of Oracle configuration screens as supporting evidence. This approach was inefficient because screenshots were difficult to standardize, review, and trace across multiple entities and reporting periods. By converting configuration verification into structured system-generated reports, the framework improved both audit readability and consistency while reducing the risk of incomplete or inconsistent evidence submission.

3.3 Module 3: Self-Service Inquiry Model and Digital Trust

An important architectural feature of the framework was the introduction of a controlled self-service inquiry model through a custom Oracle responsibility named "SFDC SOX Inquiry." The design followed the principle of Least Privilege, ensuring that eGRC auditors could execute required reports and access compliance evidence without receiving full administrative privileges within the ERP system [7].

This separation was strategically important for maintaining digital trust and governance integrity. In many organizations, the same technology teams responsible for maintaining ERP configurations are also asked to support audit evidence collection, creating potential conflicts of interest. The self-service inquiry model established a clearer separation between system administrators and auditors by allowing compliance teams to independently retrieve evidence while preserving strict access boundaries.

By embedding controlled self-service access directly into Oracle EBS, the framework strengthened transparency and reduced dependence on technical teams for recurring compliance requests. This not only improved operational efficiency but also reinforced governance principles by ensuring that the "builders" of the system and the "auditors" of the system remained functionally separated within the enterprise control environment.

4. RESULTS AND EMPIRICAL IMPACT

The framework was institutionalized across the finance and payroll business teams. The measurable outcomes are summarized in Table 1.

Table 1. Comparative Analysis of Compliance Workflows

Metric	Manual Baseline	Automated Framework	Improvement
Execution Time	40 Hours / Quarter	1 Hour / Quarter	97.5%
Data Integrity	Manual Screenshots	Programmatic SQL/XML	High Fidelity
Turnaround Time	3-5 Business Days	Near Real-Time	>90%
User Access	IT-Dependent	Self-Service (SOX Inquiry)	Absolute

The automation significantly reduced the redundant effort repeatedly highlighted by finance, audit, and technology stakeholders during quarterly SOX cycles. Activities that previously involved manual report extraction, screenshot capture, validation, and evidence compilation were streamlined into a centralized automated workflow, eliminating much of the repetitive administrative workload associated with compliance reporting. This improvement aligns with recent findings that organizations adopting targeted SOX control automation have reduced audit-related effort by more than 30%, allowing internal audit teams to redirect their focus toward complex risk analysis and governance activities rather than routine evidence collection [8].

For the organization, the operational impact was substantial. The SOX certification closure timeline was reduced by 97.5%, shrinking a process that once consumed nearly 40 hours into a workflow that could be completed in approximately one hour. Beyond the measurable efficiency gains, this shift freed the technology services team from recurring compliance-support tasks and allowed greater focus on strategic ERP modernization initiatives, including the broader transformation roadmap involving cloud-based platforms such as Workday and Zuora.

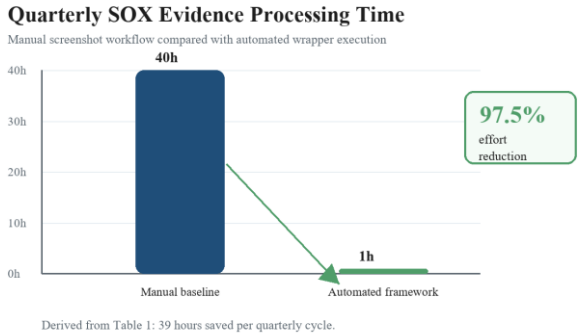

Figure 1. Quarterly SOX evidence processing time before and after automation.

Figure 1 visually emphasizes the principal empirical finding: the wrapper framework compressed quarterly SOX evidence preparation from approximately 40 hours to approximately 1 hour, representing a 97.5% reduction in recurring effort.

4.1 Operational Efficiency Analysis

The quantitative result shows a reduction from approximately 40 hours to approximately 1 hour per quarterly SOX certification cycle. This is equivalent to 39 hours saved per cycle and about 156 hours annually for the same recurring evidence-preparation workflow. The magnitude of the reduction indicates that the main efficiency gain came from eliminating repeated navigation, screenshot collection, file consolidation, and manual evidence-upload activities rather than from simply accelerating a single report.

Analytically, this changes the cost structure of compliance. Under the manual model, effort increases almost linearly as the number of controls, ledgers, business units, and reporting periods expands. Under the wrapper model, incremental evidence requests can be absorbed through reusable concurrent programs and standardized output packages. The fixed cost moves to design, testing, change control, and periodic maintenance, while recurring audit-cycle effort shifts toward exception review and evidence interpretation.

4.2 Evidence Reliability and Audit Traceability Analysis

The research also indicates a qualitative improvement in evidence reliability. Manual screenshots capture a screen state but do not always expose the query logic, completeness of the population, extraction timestamp, or underlying data relationships. Programmatic SQL/XML evidence offers a more auditable artifact because the data fields, parameters, and execution outputs can be standardized across periods.

From an audit-traceability perspective, standardized extracts create a clearer evidence chain from system configuration to reviewer conclusion. Bank-account extracts, ledger approval validations, user listings, responsibility-by-function reports, and fixed-asset configuration reports become comparable across quarters. This improves repeatability and reduces reviewer ambiguity because each control can be supported by

the same data structure instead of by inconsistent screenshots prepared by different users.

Table 2. Analytical Interpretation of Automation Outcomes

Dimension	Detailed analysis
Time reduction	The 97.5% improvement reflects removal of recurring manual tasks and supports a shift from administrative audit preparation to analytical control review.
Evidence quality	SQL/XML outputs improve reproducibility, completeness, and field-level traceability compared with screen captures.
Governance model	The SFDC SOX Inquiry responsibility supports least-privilege access while reducing dependence on technical teams for routine evidence retrieval.
Scalability	Additional reports can be attached to the wrapper architecture, allowing a modular expansion path for other SOX and ITGC controls.
Research limitation	The measured outcome is implementation-based evidence from one enterprise setting; broader validation would require multi-period and multi-organization comparison.

4.3 Governance and Control-Design Analysis

The self-service inquiry model is significant because SOX evidence gathering often creates a tension between operational ownership and audit independence. When the same technology team that configures ERP controls is also responsible for producing recurring audit evidence, independence can appear weakened even when no improper activity has occurred. The controlled inquiry responsibility reduces that tension by enabling eGRC auditors to obtain evidence directly while preserving access boundaries.

However, automation should be interpreted as a control-enhancement mechanism rather than a replacement for governance. Wrapper programs require their own control environment, including change-management approval, restricted developer access, version tracking, output reconciliation, and periodic validation of report logic. Without these safeguards, an automated evidence tool could reproduce incorrect logic at scale. The framework therefore creates value when automation is paired with disciplined ITGC oversight.

4.4 Scalability, Boundary Conditions, and Research Implications

The architecture has scalability potential because it uses modular report execution rather than a one-off evidence script. Controls that share common audit attributes, such as configuration parameters, approval indicators, user responsibilities, and system-generated timestamps, can be integrated into the wrapper model with limited changes to the user-facing process. This supports the movement from episodic evidence preparation toward a more continuous SOX-readiness posture.

At the same time, the findings should be interpreted within clear boundary conditions. The reported 97.5% reduction is tied to the studied workflow, its baseline manual effort, and the maturity of the Oracle EBS reporting environment. Organizations with different control volumes, ERP customizations, data-quality constraints, or approval workflows may experience different results. Future empirical research could compare multiple quarters, multiple ERP modules, and multiple organizations to test whether similar automation architectures produce consistent improvements in audit effort, evidence quality, and control assurance.

The broader research contribution is that SOX automation is framed not only as process optimization but also as evidence architecture. The framework demonstrates how compliance artifacts can be generated as structured system outputs, governed through role-based access, and reviewed through standardized analytical dimensions. This supports a stronger connection between ERP governance, continuous monitoring, and financial-reporting reliability.

4.5 Extended Evaluation Across Datasets and Scenarios

A more extensive evaluation can further strengthen the research by testing the automation framework across multiple compliance datasets rather than relying only on the aggregate quarterly effort reduction. The framework is especially suitable for scenario-based evaluation because each wrapper output represents a distinct control-evidence population, such as bank-account configuration data, ledger approval settings, user-access listings, responsibility-by-function mappings, and fixed-asset setup records. Evaluating these datasets separately would help determine whether the observed efficiency gains are consistent across financial, access-control, and configuration-control domains.

The expanded evaluation should also compare routine audit cycles with higher-risk scenarios, including high-volume user-access reviews, quarter-end evidence refreshes, configuration changes after system releases, and cross-platform transformation activities involving Oracle EBS, Workday, and Zuora. Such scenario testing would improve external validity by showing whether the wrapper architecture remains reliable when control volume, data complexity, review urgency, or system-change activity increases.

Table 3. Proposed Multi-Scenario Evaluation Matrix

Dataset or scenario	Evaluation focus and analytical value
Bank-account and cash-management extracts	Tests completeness of account setup evidence, branch-level configuration capture, extraction time, and reduction in manual screenshot validation.
Ledger approval and journal-control data	Evaluates whether approval-enabled ledgers are identified consistently across periods and whether exception review becomes more traceable.
User listing and responsibility-by-function datasets	Measures population coverage, role-to-function traceability, and support for Segregation of Duties and ITGC review.
Fixed-asset configuration records	Assesses repeatability of depreciation-method, prorate-convention, and asset-calendar evidence across reporting periods.
High-volume or exception-heavy audit cycle	Examines scalability under increased control volume by comparing runtime, reviewer rework, exception rate, and evidence-packaging consistency.
ERP modernization and cloud-transition scenario	Analyzes how Oracle EBS evidence requirements can be mapped to related governance needs during Workday and Zuora transformation activities.

This broader evaluation design would allow future studies to move beyond a single before-and-after efficiency measure. It would support comparative analysis across datasets, reveal which control categories benefit most from automation, and identify where human review remains essential. The resulting evidence would make the research more generalizable because the framework would be assessed not only by time saved, but also by completeness, repeatability, exception visibility, audit acceptance, and scalability under changing enterprise conditions.

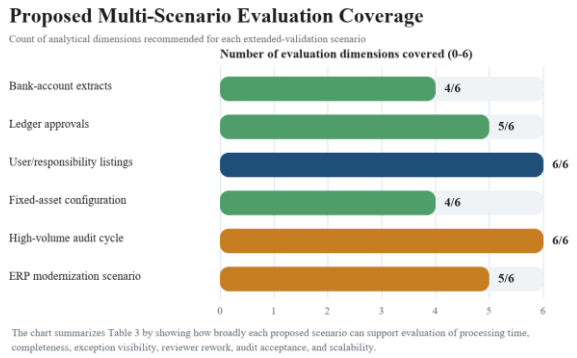

Figure 2. Proposed evaluation coverage across datasets and analytical dimensions.

Figure 2 complements Table 3 by presenting the expanded evaluation as a visual coverage chart. The figure clarifies how future research can assess the framework across financial-control, ITGC, fixed-asset, high-volume audit, and transformation scenarios.

5. CONCLUSION AND FUTURE WORK

This study demonstrates that the traditional "screenshot-and-verify" approach to SOX compliance is increasingly unsustainable in modern, high-volume enterprise environments. As organizations continue to scale their financial operations and accelerate digital transformation initiatives, manual evidence gathering creates operational inefficiencies, delays audit readiness, and places unnecessary pressure on finance and technology teams. The implementation of the SOX Automation Wrapper framework showed that compliance activities can be embedded directly within the ERP ecosystem through standardized, program-driven extraction and reporting mechanisms. By replacing fragmented manual workflows with automated evidence generation, the organization significantly reduced compliance effort while improving consistency, traceability, and internal control reliability.

The detailed analysis further indicates that the framework's value comes from four mutually reinforcing mechanisms: time compression, evidence standardization, controlled auditor self-service, and modular scalability. These mechanisms collectively strengthen audit readiness while keeping vendor-specific ERP controls intact.

Beyond operational efficiency, the framework also highlights the broader strategic value of "In-ERP" governance automation. The solution strengthened SOX compliance, improved audit transparency, reduced dependency on repetitive administrative work, and allowed technology resources to focus more actively on enterprise modernization initiatives. The study therefore reinforces the idea that effective compliance automation is not merely a cost-saving exercise, but an important component of long-term digital governance strategy.

Future empirical work should therefore validate the framework across additional datasets, multiple quarterly cycles, and different control scenarios. A multi-scenario evaluation would allow researchers to compare processing time, data completeness, exception volume, reviewer rework, and audit acceptance across financial-control, ITGC, fixed-asset, and access-governance datasets.

Future research can extend this framework by integrating Generative AI and Large Language Models (LLMs) into eGRC platforms. While the current system automates evidence extraction and reporting, emerging AI-driven approaches could enable intelligent anomaly detection, predictive compliance monitoring, and proactive remediation recommendations. Such systems may eventually move organizations beyond reactive audit preparation toward fully adaptive, continuously monitored compliance environments capable of identifying control risks before they materialize into audit issues.

6. REFERENCES

[1] M. Alles and G. L. Gray, "Incorporating continuous monitoring into ITGC: A roadmap for SOX compliance," Journal of Information Systems, vol. 30, no. 1, pp. 145–165, 2016.

[2] J. E. Hunton, A. M. Wright, and S. G. Wright, "Are financial officers concerned about control and audit in the era of continuous monitoring?" International Journal of Auditing, vol. 12, no. 1, pp. 25–41, 2008.

[3] S. H. Hassan, "Enhancing audit quality and reducing costs: the impact of AI in banking and financial services," PMC - National Center for Biotechnology Information, Jan. 2026.

[4] R. Debreceny, G. L. Gray, J. J. J. Ng, K. S. P. Lee, and W. F. Yau, "Embedded audit modules in ERP systems: Implementation and functionality," Journal of Information Systems, vol. 19, no. 2, pp. 7–27, 2005.

[5] R. B. Potla, "A SOX/ITAR-Aligned Global ERP Template for Multi-Plant Manufacturers: Governance Patterns and Controls," Journal of Artificial Intelligence, Machine Learning and Data Science, vol. 2, no. 2, pp. 3222–3232, 2024.

[6] B. S. L. G. L. Gray et al., "Measuring the pervasiveness of IT general controls: A model and empirical validation," International Journal of Accounting Information Systems, vol. 56, 2025.

[7] AICPA, "The impact of SOC 1 and SOC 2 reports on financial statement audits," Journal of Accountancy, 2021.

[8] KPMG, "KPMG SOX Report: Modernizing the SOX Program with Automation," 2023.

[9] M. Eulerich, N. Waddoups, M. Wagener, and D. A. Wood, "Development of a Framework of Key Internal Control and Governance Principles for Robotic Process Automation (RPA)," Journal of Information Systems, vol. 38, no. 2, pp. 29–49, 2024.