World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Understanding risks when implementing security and controls for SOX applications

Sujan Kumar Seethamsetty Venkata *

Senior Manager, USA.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(02), 1048-1056

Publication history: Received on 28 March 2025; revised on 06 May 2025; accepted on 09 May 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.2.0642

Abstract

This article explores the multifaceted risk landscape organizations face when implementing security and controls for Sarbanes-Oxley (SOX) compliance. Drawing on industry research and case studies, it examines the operational, financial, compliance, and technology risks that emerge during SOX implementation initiatives. The article identifies critical vulnerabilities in access controls, data integrity, process inefficiencies, and monitoring mechanisms that can undermine compliance efforts. It outlines structured approaches to risk mitigation through assessment frameworks, control prioritization, continuous monitoring, and technical implementations. Additionally, the article emphasizes the importance of cross-functional collaboration between IT, audit, management, and business process owners to achieve sustainable compliance. Through real-world case studies, it contrasts a manufacturing company's problematic implementation with a financial services firm's successful approach, extracting valuable lessons for organizations navigating similar compliance challenges. The comprehensive article provides a roadmap for transforming SOX compliance from a regulatory burden into a strategic advantage that enhances overall security posture while meeting regulatory requirements.

Keywords: SOX Compliance; Risk Management; Internal Controls; Financial Reporting; Cross-Functional Collaboration

1. Introduction

The Sarbanes-Oxley Act of 2002 transformed corporate governance and financial reporting in the United States. Enacted in response to major accounting scandals at companies like Enron and WorldCom, SOX introduced stringent requirements for internal controls over financial reporting (ICFR). Section 404 of SOX specifically mandates that management assess and report on the effectiveness of these controls, while external auditors must attest to management's assessment.

For IT departments, SOX compliance presents unique challenges. Protiviti's 2023 SOX compliance survey reveals that organizations continue to experience rising costs and complexity in their compliance efforts, with digital transformation and cybersecurity initiatives significantly impacting the scope of SOX programs [1]. The implementation of controls for financial applications and systems must be robust enough to satisfy regulatory requirements while remaining practical for day-to-day operations. The survey indicates that organizations are increasingly integrating ESG risks into their SOX compliance frameworks and emphasizing the importance of IT general controls in financial reporting.

This balancing act introduces numerous risks that, if not properly managed, can lead to compliance failures, operational disruptions, and financial losses. According to Audit Analytics's seventeen-year review of SOX 404 disclosures, ineffective internal controls remain a persistent challenge, with many organizations reporting material weaknesses related to IT controls [2]. The study shows a correlation between internal control deficiencies and subsequent financial restatements, highlighting the critical importance of effective IT governance in maintaining financial reporting integrity.

* Corresponding author: Sujan Kumar Seethamsetty Venkata

This article explores the risk landscape of SOX implementation, offering technical insights and strategic approaches to security control deployment. By understanding these risks and adopting appropriate mitigation strategies, organizations can achieve compliance objectives while enhancing their overall security posture. The increasing adoption of automation and advanced technologies in SOX compliance programs demonstrates a growing recognition that proactive risk management can transform compliance from a burdensome requirement into a strategic advantage [1].

2. Types of Risks in SOX Implementation

When deploying security and controls for SOX applications, organizations face multiple categories of risk that require careful consideration:

2.1. Operational Risks

Operational risks stem from inefficiencies in business processes resulting from control implementation. Workflow disruption occurs when overly restrictive controls impede legitimate activities, creating bottlenecks. According to Plante Moran, organizations frequently encounter operational delays when controls are implemented without considering actual business workflows, resulting in redundant approvals [3]. System performance can degrade from security measures such as comprehensive logging and encryption. Change management challenges arise when implementing new controls as they necessitate changes to established workflows. Resource allocation issues emerge as dedicating personnel to SOX compliance diverts resources from other critical IT initiatives.

2.2. Financial Risks

The financial implications of SOX control implementation are substantial. Implementation costs for deploying robust security measures require significant investment, with Zluri reporting that public companies spend an average of $1-2 million annually on SOX compliance, with technology controls representing approximately 30% of these costs [4]. Remediation expenses add another burden when addressing control deficiencies identified during audits, especially under tight deadlines. Audit failures present a significant risk, as inadequate controls can lead to material weaknesses reported by auditors. AuditBoard notes that companies disclosing material weaknesses often experience negative market reactions and increased scrutiny from regulators [5]. Non-compliance can result in severe financial penalties, with executives facing personal liability.

2.3. Compliance Risks

Compliance risks relate directly to regulatory requirements. Regulatory interpretation challenges arise as organizations struggle to translate broad principles into specific control requirements. Plante Moran highlights that organizations frequently implement unnecessary controls due to misinterpretation of SOX requirements, increasing costs without proportional risk reduction [3]. Scope creep occurs when organizations expand their control environments beyond necessary boundaries. Documentation deficiencies constitute a persistent challenge, as insufficient documentation can lead to compliance failures even when actual controls are adequate. Framework alignment issues complicate efforts as organizations struggle to map controls to recognized frameworks like COSO or COBIT.

2.4. Technology Risks

Technology-specific risks present unique challenges in SOX compliance. System integration complications arise when implementing controls across disparate systems. Zluri emphasizes that organizations with complex technology ecosystems face significantly higher compliance costs, with integration challenges accounting for approximately 25% of SOX technology spending [4]. Legacy system limitations pose obstacles, as older applications often lack modern security features needed for compliance. AuditBoard reports that while automation can reduce compliance costs by up to 25%, poorly implemented automated controls can create single points of failure [5]. Emerging technology challenges continue to evolve as organizations adopt cloud services and remote work environments, introducing new compliance complexities.

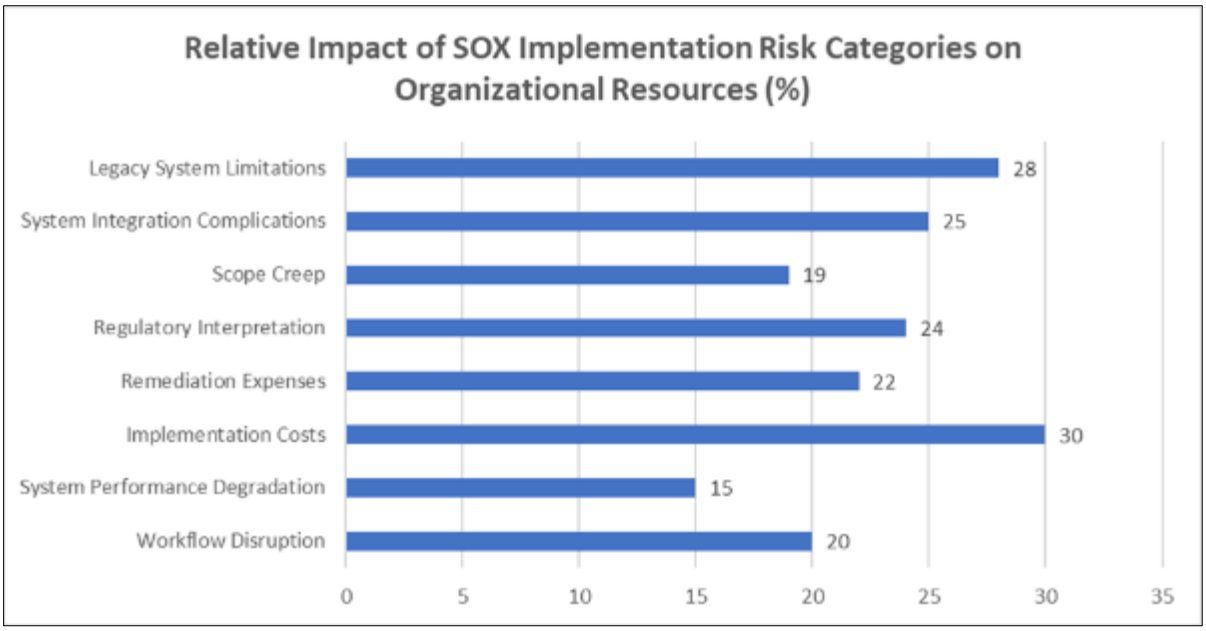

Figure 1 Comparative Analysis of Financial, Operational, Compliance, and Technology Risks in SOX Implementation [3, 4]

3. Identifying Vulnerabilities in SOX Controls

Effective risk management begins with identifying specific vulnerabilities that could compromise SOX compliance. Key areas of vulnerability include:

3.1. Access Control Vulnerabilities

Access controls represent a primary focus of SOX compliance, with several common vulnerabilities. Segregation of Duties (SoD) conflicts constitute a significant risk, as inadequate separation of critical financial functions can enable fraud. According to Deloitte's SOX program assessment framework, organizations with mature control environments implement systematic SoD analyses that identify potential conflicts before they manifest in financial processes [6]. Excessive privileges present another major vulnerability, as over-provisioning of access rights, particularly for administrative accounts, expands the attack surface for potential data manipulation. EY's Global Information Security Survey found that access control deficiencies remain among the top three security vulnerabilities in financial systems, with privileged account management presenting particular challenges [7]. Orphaned accounts create persistent security gaps when organizations fail to promptly deactivate access for terminated employees. Such accounts remain a significant threat vector, especially in organizations without automated deprovisioning workflows. Inadequate authentication mechanisms, including weak password policies, lack of multi-factor authentication, and insufficient access review processes, further undermine control integrity. Third-party access issues compound these vulnerabilities, as vendor access to financial systems often lacks proper oversight and monitoring. PwC's Digital Trust Insights research highlights that third-party access controls often receive less scrutiny than internal controls despite representing significant potential entry points for unauthorized access [8].

3.2. Data Integrity Vulnerabilities

SOX compliance depends fundamentally on data integrity within financial systems. Data validation weaknesses represent a critical vulnerability when insufficient input validation controls allow erroneous or fraudulent data to enter financial systems. Change control deficiencies threaten data integrity when organizations implement inadequate controls over modifications to financial data, particularly direct database changes outside application controls. Deloitte's modernization framework for SOX programs emphasizes the critical importance of comprehensive change management procedures, noting that organizations with formalized change control processes experience significantly fewer data integrity issues [6]. Backup and recovery limitations create significant risks when organizations cannot restore accurate financial information after corruption or loss. Data classification gaps frequently emerge when organizations fail to identify and protect sensitive financial data, increasing unauthorized access risks. EY's survey indicates that fewer than half of organizations maintain comprehensive data classification schemes that adequately identify and protect financial data subject to SOX requirements [7]. Interface control issues arise when weak controls

over data transfers between systems allow unauthorized modifications during transmission, with integration points representing particular vulnerability areas for data integrity compromises.

3.3. Process Inefficiencies

Procedural vulnerabilities can undermine even well-designed technical controls. Manual control overreliance creates significant risks as excessive dependence on manual processes increases the likelihood of human error and inconsistent application. Organizations with heavily manual control environments experience substantially higher error rates compared to those with automated controls. Unclear control ownership creates accountability gaps when responsibility for control execution and monitoring remains ambiguous. Inadequate testing before implementation may result in controls that fail to address actual risks or cause unexpected operational disruptions. According to EY's security maturity assessment methodology, pre-implementation testing remains an underdeveloped practice in approximately 60% of organizations implementing SOX controls [7]. Control obsolescence represents another significant vulnerability as controls that aren't regularly reviewed and updated become ineffective as business processes, systems, or threats evolve. Incident response deficiencies extend the impact of breaches when organizations lack adequate procedures for addressing control failures or security incidents, with Deloitte recommending that SOX programs incorporate incident response capabilities specifically designed for financial control failures [6].

3.4. Monitoring and Oversight Weaknesses

Continuous monitoring is essential for maintaining SOX compliance. Audit trail limitations present significant vulnerabilities when insufficient logging of system activities and financial transactions hinders investigation of potential fraud or errors. Alert fatigue emerges when excessive or poorly tuned monitoring alerts lead to important warnings being ignored or overlooked. PwC's survey findings reveal that organizations struggle to balance comprehensive monitoring with manageable alert volumes, with many reporting that alert overload contributes to delayed identification of control issues [8]. Inadequate metrics for measuring control effectiveness prevent organizations from identifying deteriorating controls before failures occur. Organizations utilizing quantitative metrics to measure control performance typically detect control degradation earlier than those relying solely on qualitative assessments. Reporting deficiencies create vulnerabilities when ineffective reporting mechanisms prevent timely escalation of control issues to appropriate management levels, with Deloitte's assessment methodology highlighting efficient escalation paths as a key differentiator between high-performing and struggling SOX programs [6].

Table 1 Critical Vulnerabilities in SOX Control Environments: Detection Difficulty vs. Remediation Complexity [5, 6]

Vulnerability Category	Specific Vulnerability	Prevalence/Impact	Detection Difficulty (1-5)	Remediation Complexity (1-5)
Access Control	Segregation of Duties Conflicts	High	3	4
	Excessive Privileges	Very High	2	3
	Orphaned Accounts	Medium	2	1
Data Integrity	Data Validation Weaknesses	High	3	3
	Change Control Deficiencies	Very High	4	4
	Backup/Recovery Limitations	Medium	2	3
Process Inefficiencies	Manual Control Overreliance	High	2	4
	Unclear Control Ownership	Medium	3	2
	Inadequate Testing	Very High	3	3
Monitoring & Oversight	Audit Trail Limitations	High	3	4
	Alert Fatigue	Medium	4	3

4. Risk Mitigation Strategies

Addressing the complex risks associated with SOX compliance requires a structured approach to risk mitigation:

4.1. Risk Assessment Frameworks

Implementing formal risk assessment methodologies provides a foundation for effective risk management. Risk mapping represents a crucial first step, involving the systematic identification and documentation of relationships between financial reporting risks, processes, systems, and controls to ensure comprehensive coverage. According to Pathlock's practical guide on internal controls for SOX compliance, organizations that implement comprehensive risk mapping can better identify control gaps and redundancies, leading to more efficient compliance programs and reducing the risk of material weaknesses [9]. Quantitative risk analysis enhances this approach by assigning numerical values to risks based on likelihood and potential impact, enabling organizations to prioritize mitigation efforts for highest-risk areas. This quantification allows for more objective decision-making about control investments and resource allocation.

Control maturity assessment provides another critical framework component by evaluating existing controls against established maturity models like CMMI (Capability Maturity Model Integration). This evaluation helps identify improvement opportunities and establish realistic roadmaps for control enhancement. Organizations typically progress through defined maturity levels, from initial ad-hoc controls to optimized, continuously improving control environments. Threat modeling complements these approaches by applying formal techniques to financial applications, identifying potential attack vectors and control requirements. Zluri's best practices guide emphasizes that organizations implementing formal threat modeling as part of their SOX compliance programs can identify potential vulnerabilities earlier in the development lifecycle, reducing remediation costs [10].

A sample risk assessment matrix illustrates this approach:

Table 2 SOX Implementation Risk Assessment Matrix: Likelihood and Impact Analysis [7, 8]

Risk Category	Likelihood (1-5)	Impact (1-5)	Risk Score	Priority
Unauthorized access to financial data	4	5	20	High
System downtime during financial close	3	4	12	Medium
Segregation of duties conflict	4	4	16	High
Inadequate change management	3	3	9	Medium
Data integrity compromise	2	5	10	Medium

4.2. Control Prioritization

With limited resources, organizations must prioritize control implementation strategically. Critical path analysis involves identifying controls that directly impact the most significant financial reporting risks and prioritizing their implementation. Pathlock's practical guide emphasizes the importance of using a risk-based approach to prioritize efforts on the most critical controls, focusing on those that address key financial assertions and significant accounts that pose the highest risk of material misstatement [9]. This distinction helps organizations focus resources where they will have the greatest impact on compliance and risk reduction.

Control hierarchy implementation establishes a logical sequence for control deployment, ensuring that foundational controls are in place before more advanced measures. This hierarchical approach recognizes that basic security requirements must be met before addressing more complex scenarios. For example, fundamental access controls should be established before implementing sophisticated data loss prevention systems. Compensating control strategy provides flexibility when primary controls cannot be immediately implemented, allowing organizations to deploy alternative measures to mitigate risks in the interim. Zluri recommends documenting these compensating controls with clear rationales and establishing timelines for implementing permanent solutions [10].

Quick win identification targets high-impact, low-effort controls for early implementation, demonstrating progress and building momentum for broader compliance initiatives. These quick wins generate organizational support by showing tangible benefits while laying groundwork for more complex control implementations. Organizations that begin with a balanced portfolio of quick wins and strategic controls typically achieve faster overall compliance timelines.

4.3. Continuous Monitoring Approach

Proactive monitoring enables the early detection of control weaknesses before they impact financial reporting. Real-time alerting implements automated notifications for critical control failures or suspicious activities requiring immediate attention. According to Pathlock's practical guide for SOX compliance, organizations implementing real-time alerting for key controls can significantly reduce the time to detect potential issues compared to those relying on periodic reviews, enabling more proactive risk management and timely remediation of control deficiencies [9]. This early detection significantly reduces the potential impact of control failures.

Control dashboard development creates a centralized visualization of control status across the organization, highlighting areas of risk or concern. These dashboards provide executives and control owners with an at-a-glance understanding of compliance status, trending issues, and control effectiveness. Periodic control testing establishes regular evaluation schedules for key controls to verify continued effectiveness, typically following a risk-based approach where higher-risk controls undergo more frequent testing. The exception management process formalizes procedures for reviewing, documenting, and addressing control exceptions, ensuring that deviations receive appropriate attention and remediation.

Continuous Control Monitoring (CCM) represents the most advanced approach, deploying automated tools to validate control effectiveness on an ongoing basis rather than relying solely on periodic testing. Zluri's best practices guide highlights that organizations implementing CCM can reduce manual testing efforts while improving coverage and consistency, leading to more efficient compliance programs with fewer control failures [10]. This automation allows for more comprehensive coverage with reduced manual effort, shifting resources from detection to prevention activities.

4.4. Technical Control Implementation

Specific technical measures address SOX-related risks through automation and specialized tools. Privileged Access Management (PAM) implements solutions to manage, monitor, and control privileged access to financial systems, including session recording for administrative activities. Pathlock's practical guide for SOX compliance recommends that organizations implement comprehensive PAM solutions as part of their technology enablement strategy, particularly for systems supporting financial reporting, to maintain the principle of least privilege and prevent unauthorized access to sensitive financial data [9]. These measures significantly reduce the risk of unauthorized modifications to financial data.

Identity governance deploys automated provisioning and deprovisioning workflows integrated with HR systems to ensure timely access changes, particularly for employee onboarding, role changes, and terminations. Database activity monitoring implements the surveillance of direct database access, particularly for sensitive financial tables, to detect unauthorized modifications. This monitoring provides visibility into changes occurring outside application controls, which represent a significant risk area for SOX compliance.

Change control automation leverages workflow tools to enforce approval processes and maintain audit trails for system changes, ensuring that all modifications to financial systems follow established procedures and receive appropriate authorization. According to Zluri, organizations implementing automated change management workflows experience fewer unauthorized changes to financial systems and can more easily demonstrate compliance with SOX requirements [10]. Data Loss Prevention (DLP) implements controls to prevent unauthorized exfiltration of sensitive financial data, protecting against both malicious actions and inadvertent data exposure. These technical controls, when implemented as part of a comprehensive risk management strategy, provide automated enforcement of policy requirements while generating evidence needed for SOX certification and audit activities.

5. Collaboration Across Teams

Effective SOX compliance requires cross-functional cooperation across the organization:

5.1. IT and Audit Alignment

Bridging the traditional gap between IT and audit functions represents a critical success factor for SOX implementation. Common control language development establishes shared taxonomy between teams, facilitating clearer communication. According to PwC's compliance transformation framework, organizations with standardized control definitions experience significantly fewer misinterpretations during audit processes [11]. Joint risk assessment brings together IT and audit perspectives to ensure comprehensive risk identification, with collaborative approaches identifying more potential scenarios than siloed assessments. Control design workshops provide forums where IT and

audit teams design controls together, ensuring both technical feasibility and compliance effectiveness. Deloitte's SOX readiness guide emphasizes that controls developed collaboratively are substantially less likely to require revision during external audits [12]. Audit readiness reviews complete this alignment by implementing pre-audit evaluations where teams jointly assess control evidence before external auditors arrive.

5.2. Management Engagement

Executive leadership provides the authority and resources necessary for effective SOX implementation. Executive sponsorship demonstrates organizational commitment, with PwC noting that programs with active C-suite involvement achieve compliance more efficiently [11]. Resource allocation advocacy ensures adequate budget and personnel for compliance efforts. Risk acceptance protocols establish formal processes for management acknowledgment when complete mitigation isn't feasible. Deloitte recommends tiered approval requirements based on risk severity [12]. Regular status reporting maintains executive engagement by providing actionable compliance updates that help leaders understand status without requiring technical knowledge.

5.3. Business Process Owner Integration

Engaging operational stakeholders ensures that controls remain practical within day-to-day operations. Control impact analysis collaborates with process owners to assess operational effects before implementation. PwC's research shows that organizations performing formal impact analysis experience fewer operational disruptions after control implementation [11]. User acceptance testing involves business users in identifying potential workflow issues. Process improvement alignment integrates control implementation with business improvement initiatives. Deloitte emphasizes that this integrated approach achieves cost savings compared to treating compliance and improvement separately [12]. Control ownership transfer ensures controls become embedded in normal business operations rather than remaining separate compliance activities.

Table 3 Cross-Functional Collaboration Framework for Effective SOX Compliance [9, 10]

Collaboration Area	Key Practice	Primary Benefit	Secondary Benefit
IT-Audit Alignment	Common Control Language	Fewer Audit Misinterpretations	Improved Communication
	Joint Risk Assessment	Comprehensive Risk Identification	Elimination of Siloed Approaches
	Control Design Workshops	Technical Feasibility	Reduced External Audit Revisions
	Audit Readiness Reviews	Pre-audit Evidence Assessment	Early Issue Identification
Management Engagement	Executive Sponsorship	More Efficient Compliance	Organizational Commitment
	Resource Allocation Advocacy	Adequate Budget and Personnel	Streamlined Implementation
	Risk Acceptance Protocols	Clear Management Acknowledgment	Tiered Approval Requirements
	Regular Status Reporting	Maintained Executive Engagement	Non-technical Updates
Business Process Integration	Control Impact Analysis	Fewer Operational Disruptions	Practical Control Design
	User Acceptance Testing	Early Workflow Issue Identification	Increased User Buy-in
	Process Improvement Alignment	Cost Savings	Operational Efficiency Gains
	Control Ownership Transfer	Embedded Operational Controls	Sustainable Compliance

6. Case Studies: Learning from Experience

Real-world examples provide valuable insights into both the challenges and successful approaches to SOX control implementation:

6.1. Case Study 1: Manufacturing Company's Access Control Implementation

A mid-sized manufacturing company implemented a new identity management system to address SOX access control requirements. The implementation team focused primarily on technical configuration without adequate business process analysis, creating a cautionary tale documented in RoseRyan's SOX implementation lessons learned analysis [13]. The technical focus without business alignment resulted in production delays due to restrictive approval workflows that didn't accommodate manufacturing's time-sensitive operational needs. During month-end closing periods, the company experienced hundreds of emergency access exceptions as employees required immediate system access to complete critical financial tasks, creating both compliance and security risks. The implementation also generated significant user resistance as employees found workarounds to complete their jobs, including the emergence of shadow IT practices where departments deployed unofficial tools to bypass cumbersome controls.

From this experience, several key lessons emerged that guide other organizations. First, conducting thorough business impact analysis before implementing access controls helps identify potential operational disruptions before they occur. According to Zluri's SOX compliance best practices guide, organizations should "map critical business processes and understand peak activity periods before designing approval workflows" to avoid disruptions [10]. Second, designing controls with operational efficiency in mind ensures that security measures enhance rather than impede business functions. Finally, implementing phased rollouts with feedback loops to adjust control parameters allows organizations to refine controls based on real-world usage patterns before full deployment. After experiencing significant disruption, this manufacturing company ultimately redesigned its access controls using these principles, successfully balancing compliance requirements with operational needs.

6.2. Case Study 2: Financial Services Firm's Successful Integration Approach

In contrast to the manufacturing case study, a financial services organization effectively implemented controls across a complex landscape of legacy and modern systems, as highlighted in RoseRyan's analysis of successful SOX implementations [13]. This organization approached SOX compliance strategically by first establishing a cross-functional governance committee with executive sponsorship, ensuring alignment between business, IT, and compliance objectives from the outset. The committee included senior leaders from finance, IT, operations, and risk management, creating broad organizational buy-in for the compliance initiative.

The organization developed a risk-based framework for prioritizing control implementation, focusing initial efforts on high-risk areas while developing longer-term plans for addressing medium and lower-risk domains. This approach aligns with Zluri's recommendation to "conduct a thorough risk assessment to identify and prioritize critical control areas, focusing resources where they will have the greatest impact on compliance and risk reduction" [10]. The company also created a dedicated center of excellence with specialized expertise in both financial controls and technology implementation. This team served as internal consultants to various business units, ensuring consistent control implementation while maintaining institutional knowledge. Finally, the organization implemented comprehensive continuous monitoring with meaningful metrics and dashboards, providing real-time visibility into control effectiveness.

The results of this approach were impressive and sustained. The company achieved clean SOX audits for five consecutive years, demonstrating consistent control effectiveness. They also realized a 30% reduction in compliance costs through automation and optimization of control activities, proving that effective compliance need not always increase operational expenses. Perhaps most importantly, the organization improved its overall security posture beyond SOX requirements, preventing several potential breaches through enhanced monitoring and control systems. This case demonstrates how a strategic, business-aligned approach to SOX compliance can deliver both regulatory compliance and business value.

7. Conclusion

Implementing security and controls for SOX applications requires a strategic, risk-based approach that balances regulatory requirements with operational practicality. Organizations that succeed in this balancing act view SOX compliance not merely as a regulatory obligation but as an opportunity to strengthen governance, enhance operational

efficiency, and build stakeholder trust. By systematically identifying vulnerabilities, prioritizing controls based on risk, fostering cross-functional collaboration, and implementing continuous monitoring, companies can transform compliance efforts into valuable business assets. The cases examined demonstrate that while technical implementation is important, business alignment and operational considerations are equally crucial for success. As technology landscapes evolve with cloud adoption and remote work environments, the flexibility offered by a risk-based approach provides the resilience needed to maintain compliance amidst changing conditions. Organizations that embrace these principles establish governance frameworks that extend value beyond regulatory compliance, protecting financial integrity while simultaneously enhancing their security posture and operational effectiveness in an evolving threat landscape.

References

[1] Protiviti, "The Evolution of SOX: Tech Adoption and Cost Focus Amid Business Changes, Cyber and ESG Mandates," Protiviti Inc.. [Online]. Available: https://www.protiviti.com/sites/default/files/2023-09/2023-sox-compliance-survey-protiviti.pdf

[2] Audit Analytics, "SOX 404 Disclosures: A Seventeen-Year Review," Audit Analytics, 2021. [Online]. Available: https://www.auditanalytics.com/doc/SOX_404_Disclosures_A_Seventeen-Year_Review.pdf

[3] Amanda Carrigan, Bryan O'Neill, and Caroline Smythe, "SOX compliance: Challenges boil down to people, process, technology issues," 2022. [Online]. Available: https://www.plantemoran.com/explore-our-thinking/insight/2021/10/sox-compliance-challenges-boil-down-to-people-process-technology-issues

[4] Minu Joseph, "The Cost Of SOX Compliance In 2025," 2024. [Online]. Available: https://www.zluri.com/blog/cost-of-sox-compliance

[5] Vice Vicente, "What is SOX Compliance? 2025 Complete Guide," 2024. [Online]. Available: https://www.auditboard.com/blog/sox-compliance/

[6] Deloitte, "SOX modernization: Optimizing compliance while extracting value,". [Online]. Available: https://www2.deloitte.com/us/en/pages/audit/articles/sox-program-assessment-modernization.html

[7] EY, "How does security evolve from bolted on to built-in?," 2020. [Online]. Available: https://abes.com.br/wp-content/uploads/anterior/Arquivos/Pesquisa%20EY%20-%20global-information-security-survey-2020-report.pdf

[8] Andrew Ross, "PwC's Digital Trust Insights survey results revealed," Information Age, 2019. [Online]. Available: https://www.information-age.com/pwcs-digital-trust-insights-survey-13742/

[9] Keri Bowman, "What are SOX Controls? A Practical Guide for Compliance," Pathlock, 2025. [Online]. Available: https://pathlock.com/learn/internal-controls-for-sox-compliance-a-practical-guide/

[10] Vamsi Krishna Gajula, "13 SOX Compliance Best Practices," Zluri, 2024. [Online]. Available: https://www.zluri.com/blog/sox-compliance-best-practices

[11] PwC, "Compliance Transformation," 2024. [Online]. Available: https://www.pwc.in/assets/pdfs/compliance-transformation.pdf

[12] Deloitte, "SOX Compliance: Are You Ready?". [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-audit-sox-compliance-are-you-ready.pdf

[13] RoseRyan, "8 Lessons Learned from the 2019 Sarbanes-Oxley Season to Apply This Year,". [Online]. Available: https://roseryan.com/blog/sarbanes-oxley-lessons-learned/