WHITEPAPER

Enhancing SOX Compliance

Enhancing SOX Compliance... through Effective Identity Hygiene Practices

The Sarbanes-Oxley Act of 2002 was enacted to protect investors and clients from fraudulent corporate practices, in response to a number of accounting and financial scandals. These scandals cost investors billions of dollars and shook public confidence in the US markets. The law applies to all US public company boards as well as public accounting firms.

SOX applies to all US public companies and accounting firms, requiring annual audits of financial statements and internal controls. Its 11 titles enhance corporate accountability, financial transparency, and impose stricter penalties for fraud, while establishing oversight to protect investors and the public.

From Financial Reporting to Cyber Security: Expanding SOX Compliance

SOX, initially aimed at addressing corporate fraud and improving financial reporting accuracy, has expanded to include broader IT and cybersecurity concerns due to the vital role of information systems in financial reporting. From a cyber security perspective, limiting access to financial data, along with the systems that encircle the data, is the overarching theme. That being said, an important and sometimes overlooked result, is the outcomes improve how organizations keep sensitive data safe from insider threats, cyberattacks, and data breaches.

- **What IT Systems are In Scope?** Companies should perform an analysis to identify systems critical to financial reporting, prioritizing those with access to sensitive financial data, including common IT systems such as servers, workstations, and databases.
- **Section 302: CEO/CFO Certification:** Executives are required to certify the accuracy of financial reports and ensure that effective internal controls over financial data are in place. IT systems and cybersecurity protocols directly affect the trustworthiness of financial data and organizations must ensure proper controls are operational across these systems and processes.

- **Access Controls are Essential** for ensuring only authorized personnel can access key systems. Section 404 mandates reporting on the effectiveness of these internal controls to protect data integrity and confidentiality. Important: “Personnel” doesn’t just translate to a human account anymore – there’s many human and non-human identities that can impact the integrity and confidentiality of the data.
- **If (or when) you have to disclose a breach.** If a breach compromises financial data, disclosure may be necessary under SOX. Failure to disclose, if it affects financial reporting, can lead to penalties. Disclosures should include the breach’s root cause and details on remediation efforts.

Risk management is key to SOX compliance as it helps identify and mitigate risks to financial reporting. By evaluating internal controls, companies can prevent fraud, errors, and security threats, ensuring compliance and protecting investor interests.

Although SOX doesn’t explicitly mention “cybersecurity,” cybersecurity is a critical aspect of protecting financial systems. The following section provides insights and recommendations on how to approach important assessments and remediation efforts. This includes assessing the risk, putting in controls to detect and prevent these risks from materializing into a security breach, and regularly monitoring the effectiveness of these controls.

Help Drive SOX Compliance with Identity Hygiene

Identity hygiene identifies and remediates critical identity-related issues by regularly reviewing and cleaning up access permissions, removing outdated accounts, and enforcing the principle of least privilege. This reduces the risk of unauthorized access or internal fraud, strengthening internal controls required by SOX Section 404 to ensure the accuracy and security of financial data.

Effective identity hygiene, including timely de-provisioning and regular access audits, helps companies prevent security vulnerabilities that could affect financial reporting. By managing and monitoring both end-user and privileged access, organizations can mitigate risks to financial data integrity, ensuring compliance with SOX requirements.

Access Controls

- **Least Privilege Access**: Grants users the minimum level of access needed to perform their job functions, preventing unnecessary access to sensitive systems.
  - **SOX Benefit**: Minimizes the attack surface, reducing the risk of internal fraud or errors that can affect financial reporting.
- **Access Provisioning and De-Provisioning**: Ensures that users are granted access when they join or change roles and that access is revoked promptly when they leave or no longer require access.
  - **SOX Benefit**: Ensures that only active, authorized personnel have access to financial data, reducing the risk of outdated or unnecessary access.
- **Access Review and Certification**: Regularly reviews user access rights to ensure they are still appropriate, and revokes outdated permissions.
  - **SOX Benefit**: Ensures continuous alignment between access privileges and job responsibilities, reducing risks tied to stale or excessive access.

Privileged Access Management Controls

- **Classify Privileged Accounts**: Separates privileged accounts from regular user accounts, ensuring that elevated privileges are only granted for specific, authorized tasks.
  - **SOX Benefit**: Restricts access to critical systems and data, reducing the risk of abuse by privileged users.
- **Password Rotation and Expiration**: Regularly rotates privileged account credentials and enforces expiration dates, reducing the risk of credential theft or misuse.
  - **SOX Benefit**: Protects against long-term misuse of privileged access and reduces the risk of old credentials being used to compromise financial systems.
- **Audit and Reporting for Privileged Accounts**: Provides detailed reports and logs of privileged account activities, showing which privileged users accessed what systems and when.
  - **SOX Benefit**: Enhances accountability and enables compliance audits by providing a clear trail of privileged actions affecting financial reporting.

Effective identity controls help maintain strong internal controls and reduce the risk of security incidents that could affect compliance and investor trust.

An Identity Hygiene Playbook You Can Follow

Identity Hygiene means gaining deep knowledge of your identity ecosphere, discovering all of your identities, determining their protection status, and identifying risk. It means remediating any issues—from unprotected accounts to unmanageably cluttered Active Directory (AD) estates to permission sprawl across unstructured data platforms. And it means automating discovery and remediation to keep your organization safe, now and on an ongoing basis.

Start with a Risk Assessment

- **Where To Start – There are a number of options!**
  - Determine what constitutes a "material" cybersecurity risk and which systems play a role.
  - Identify the systems and data that are in scope for SOX compliance
  - Take a risk-based approach to identifying important controls and policies

- **Review Users and Access Levels**
  - Compile a comprehensive list of all users (human and non-human) with access to in-scope systems. Include employees, contractors, and service accounts.
  - Evaluate user access permissions, focusing on privileged accounts and any users with elevated access to financial data
  - Review the organization's identity governance practices, including access provisioning, de-provisioning, and periodic access reviews.

- **Document and Report Findings**
  - Document the findings from the identity risk assessment, noting any areas of concern, vulnerabilities, or non-compliance.
  - Provide a clear report of identity-related risks to management, along with recommended actions for remediation

Identity Risk Assessment

In an identity risk assessment for SOX compliance, you should look for various identity-related risks that could compromise financial reporting integrity or violate internal controls. Key examples include:

- Excessive Privileged Access
- Outdated or Orphaned Accounts
- Lack of Segregation of Duties
- Shared Accounts
- Unmonitored Privileged Access
- Inactive or Dormant Accounts
- Non-Human Account Sprawl

Design and Implement Controls

Now that you have the Identity risks recognized, the necessary Controls should be designed and implemented to mitigate these risks in alignment with industry-accepted standards. Aligning the design and implementation of SOX compliance controls to frameworks like NIST or ISO 27001 can help standardize security practices and ensure a comprehensive approach to risk management. Below are specific controls to consider.

NIST Framework

- **Intelligent discovery**
  (NIST CSF Subcategory PR.AC-1, ID.AM-2, RS.MI-2, and more)
- **Identity, account, and group correlation**
  (NIST CSF Subcategory ID.AM-3, ID.AM-2, ID.GV-3, and more)
- **Advanced analytics and reporting**
  (NIST CSF Subcategory ID.RA-1, PR.PT-1, ID.AM-2, and more)
- **Remediation of account, group and data control violations**
  (NIST CSF Subcategory ID.BE-4, RS.MI-2, PR.AC-1, and more)
- **Sustained protection of an organization's assets**
  (NIST CSF Subcategory PR.AC-4, PR.DS-1, PR.DS-3, PR.DS-5, and more)

ISO Framework

- **Limit Account Permissions**
  (ISO 27001:2022 Annex A 5.15)
  Safeguarding access to information by ensuring employees only access what they require for their duties.
- **Monitor Access to Data**
  (ISO 27001:2022 Annex A 5.16)
  Identifying users, systems, and devices accessing data or IT assets, and managing access rights.
- **Protect Credentials from Unauthorized**
  Access (ISO 27001:2022 Annex A 5.17)
  Managing authentication information effectively to prevent breakdowns and security threats.
- **Manage Access Rights Lifecycle**
  (ISO 27001:2022 Annex A 5.18)
  Assigning, modifying, and revoking access rights in accordance with access control policies.
- **Control Elevated Privileges**
  (ISO 27001:2022 Annex A 8.2)
  Preventing misuse or abuse of elevated system administrator privileges.
- **Regulate Access to Information**
  (ISO 27001:2022 Annex A 8.3)
  Ensuring that only authorized personnel can access information.

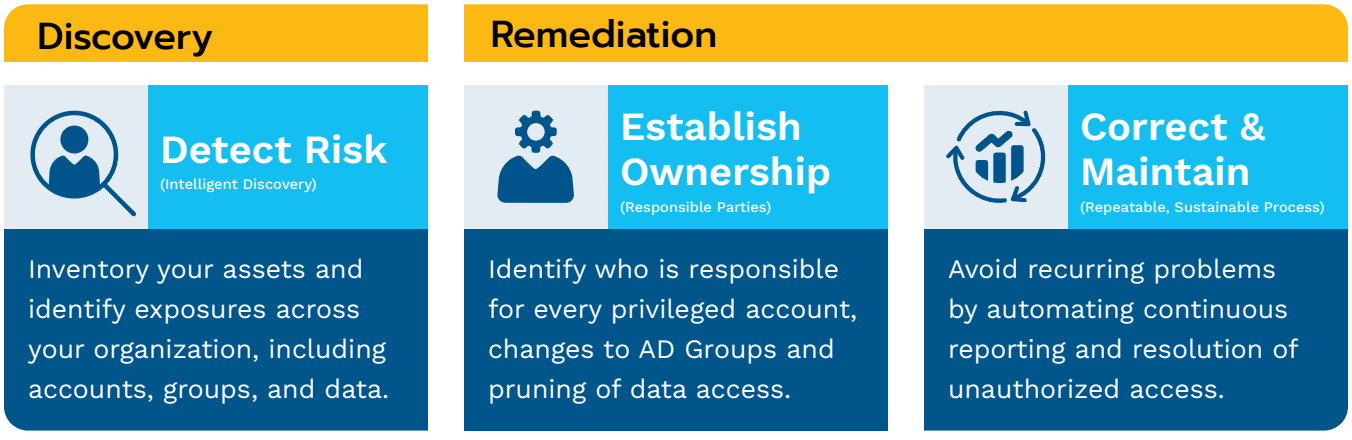
Monitor and Test Controls

Monitoring and testing controls for SOX compliance is essential to ensure that financial reporting processes remain secure and reliable. It involves regular assessments, automated monitoring, and continuous improvement efforts to confirm that the controls are working effectively.

- **Test Operating Effectiveness**
  - Sample Testing: Select a representative sample of systems and identities to verify that the control was applied correctly.
- **Automate Control Monitoring (Continuous Monitoring)**
  - Use automation to monitor key controls continuously, such as privileged access. Reduce manual efforts by automating the monitoring of critical controls, providing regular reporting for potential issues.
- **Remediate Issues**
  - Record the results of control tests and any deficiencies found. Investigate the underlying cause of the deficiency. Implement corrective actions, such as adjusting access rights or password rotating sensitive accounts.

Leverage SPHEREboard to Automate Identity Hygiene Requirements

Our SPHEREboard solutions are built on a strong foundation of sophisticated discovery and remediation capabilities—the key areas that help resolve identity-based risk. SPHEREboard helps you discover issues, prioritize risk, and establish an efficient path to risk reduction. All while introducing new automation into the process, so you can keep close watch on your environment going forward.



Summary: Enhancing SOX Compliance with Identity Hygiene

The Sarbanes-Oxley Act (SOX) was created to improve corporate accountability and protect investors by enhancing financial reporting accuracy. Initially focused on financial fraud, SOX has expanded to include IT and cybersecurity concerns, given the critical role of information systems in financial reporting. Effective access controls, as mandated by SOX, ensure only authorized personnel can access financial data, with Section 404 requiring companies to report on the effectiveness of these controls.

Identity hygiene, which involves regularly reviewing and updating access permissions, strengthens internal controls by reducing the risk of unauthorized access or fraud. By enforcing the principle of least privilege, timely de-provisioning, and regular access audits, companies can mitigate identity-related risks, ensuring SOX compliance and safeguarding the accuracy and security of financial data.

About SPHERE

SPHERE is the global leader in Identity Hygiene. We are dedicated to reshaping modern identity programs by embedding this foundational fabric, enabling organizations to quickly reduce risks. We work through an identity lens that protects an organization's accounts, data, and infrastructure. Our solutions deliver immediate time-to-value by leveraging automation to discover, remediate and secure identities, now and forever.

Driven by our core values of passion, empathy, and authenticity, our vision drives us to continually innovate, helping our clients to sleep better knowing their attack surface is drastically reduced, thwarting the plans of bad actors every single day.

We're ready to help you address your Identity Hygiene and security challenges. To find out more about SPHERE and our solutions, please visit www.sphereco.com.

