SailPoint

WHITE PAPER

Get Compliant and Stay Compliant

Best Practices for Identity Governance

This paper outlines key requirements of compliance mandates and provides recommendations on how to build a sustainable identity program to meet those requirements. It also presents a step-by-step methodology and timeline for implementing identity governance.

Organizations around the globe are confronting the reality that regulatory compliance is now a factor of everyday business life. Escalating security and privacy concerns are having a worldwide impact. There are now dozens of government and industry laws pertaining to security and privacy, forcing organizations to adhere to a complex and often overlapping series of requirements that impact almost every part of the organization. To ensure they have adequate controls necessary for compliance, organizations must be able to answer the following questions:

- Are we adequately safeguarding information assets and sensitive data?
- Can we detect and prevent fraud, misuse or unauthorized access?
- Can we safely attest to the adequacy of internal controls?
- Can we meet and prove compliance?

Effectively managing compliance has become a top issue for executive management. Many organizations invest significant time and money on compliance, yet find their investments have not resulted in effective compliance processes or policies. The cost of compliance, impact on the mission and the burden on mission support and technology departments is escalating. Worse still, many organizations have failed to adequately address actual mission risk in their compliance and governance initiatives.

First, you must understand the common regulatory requirements that public and private organizations face in order to manage information security risk and focus on the key role identity governance plays in meeting those requirements. Then, you must learn how to build a sustainable approach to compliance with an integrated set of controls across all identity business processes.

Regulatory Compliance Today: The Spotlight on Information Security

Experts agree that the regulatory compliance burden is here to stay and very likely will escalate as time goes on. Regulations like the Federal Information Security Management Act (FISMA), the Sarbanes-Oxley Act (SOX) and the Healthcare Insurance Portability and Accountability Act (HIPAA) were put in place to protect employees, shareholders, consumers and citizens from corporate fraud, data breaches and violations of privacy. These laws and similar regulations around the world – such as the General Data Protection Regulation (GDPR) – impose rigorous demands on organizations to demonstrate compliance in terms of information security and data protection.

One area of particular concern to CIOs, CISOs and other security and risk personnel is identity management: the area of IT that focuses on managing worker access to corporate systems, applications and data. Achieving transparency and managing risk around identity management requires organizations to inventory, analyze and understand the access privileges granted to their workers – and to be ready to, at any time, answer the critical question: "Who has access to what?" Failure to effectively manage user access to sensitive resources places companies at increased risk for sabotage, fraud and data breaches.

In today's world, employees, contractors, partners and even consumers require access to strategic applications and data, which could reside on-premises or in the cloud. As a result, it's becoming more challenging for organizations to ensure that workers' access is appropriate and complies with business, legal and regulatory policy. Without enterprise-wide visibility and control over users and their access, organizations will have serious gaps in their ability meet regulatory requirements.

The Right Approach to Compliance

Organizations must approach compliance requirements with sustainability in mind if they are to manage their risk effectively. If they do nothing more than what's necessary to pass a SOX or FISMA audit, they are not likely to address the entire set of operational risks or security requirements facing the organization. Effectively managing risk requires meaningful diligence above and beyond "check the box" compliance. Achieving a sustainable level of transparency and risk management to protect against the very real security threats that exist inside the organization is the true goal.

The table on the next page describes common compliance requirements facing U.S. organizations. The shared intent of the mandates shown is to prevent breaches and fraudulent or negligent behavior that could violate privacy or affect the fidelity of information assets.

U.S. Regulations Governing Privacy and Information Security

REGULATION	ORGANIZATIONS AFFECTED	FOCUS	INFORMATION SECURITY REQUIREMENTS
Sarbanes-Oxley Act (SOX)	All public companies traded on U.S. exchanges (including international companies)	Information Integrity	Ensure the accuracy of financial information and the reliability of systems that generate it. Section 404 requires management to assess internal controls and obtain attestation from external auditors annually.
Security Management Act (FISMA)	Federal agencies and affiliates	Information Integrity	Develop, document and implement programs to secure data and information systems supporting agency operations and assets.
General Data Protection Regulation (GDPR)	All organizations who conduct business in the European Union	Privacy	Protect consumer data from theft and fraud. Notify all involved parties when a breach occurs within 72 hours and "forget" cusomer data when requested.
Payment Card Industry (PCI) Data Security Standard	All members, service providers and merchants that store, process or transmit cardholder data	Fraud Prevention, Privacy	Meet 14 information security requirements in areas such as data protection, access control, monitoring and intrusion protection.
Health Insurance Portability and Accountability Act (HIPAA)	U.S. healthcare providers, payers, clearing houses and their business associates	Privacy	Protect the security and privacy of personally identifiable health information from unauthorized access, alteration, deletion or transmission.
Gramm-Leach-Bliley Act (GLBA)	U.S. based financial institutions	Privacy	Establish administrative, physical and technical safeguards to protect the security, confidentiality and integrity of consumer financial information.
North American Electric Reliability Council (NERC)	All entities responsible for planning, operating and using the bulk electric system in North America	Critical Infrastructure Protection	Protect IT assets essential to the reliability of the bulk electric system, including monitoring, access control and change/configuration management.
CA Senate Bill (SB) 1386 and 46 other state regulations	Organizations that store personal data	Privacy	Alert individuals when personal data is lost or stolen.

Taking the right approach to compliance can enable an organization to manage it as a sustainable ongoing process rather than a one-time event and to build risk management into their compliance processes.

Sustainable Compliance

To proactively address their compliance requirements, organizations should look to identity governance solutions. Identity governance is a cross-organizational, enterprise discipline that provides the intelligence and business insights needed to strengthen controls and protect information assets. With identity governance, organizations gain 360-degree visibility into and control over "who has access to what." This provides the transparency needed to reduce potential security and compliance exposures and liabilities.

Identity governance also helps organizations improve efficiency by replacing paper-based and manual processes with automated tools. Not only can an organization significantly reduce the cost of compliance, it's possible to also establish repeatable practices for a more consistent, auditable and reliable process. Taking an automated approach helps to build predictability and repeatability into the compliance tasks and workflows while also helping an organization to respond more rapidly to control weaknesses and detected violations.

The following steps describe a methodology and timeline for implementing identity governance.

The Path Towards Sustainable Compliance

The key to success is defining measurable steps to build a repeatable, sustainable compliance process across all identity tasks and activities.

1	2	3	4	5
Assess Your Current State	**Build Governance Model**	**Automate Detective Controls**	**Automate Preventive Controls**	**Perform Closed Loop Audit on All Changes**
Aggregate & Correlate Identity Data	Define Policy Model	Access Certifications	Access Request Management	Aggregate Data
Conduct Baseline Access Certification	Define Role Model	Policy Detection & Remediation	Password Management	Identify Exceptions
	Define Risk Model		Automated Provisioning	Provide Proof of Compliance

Step 1

Achieving Cross-Organization Visibility

The starting point for any identity governance project should be to understand the current state of user access within the organization by centralizing identity data. This stage involves creating a single repository for user and access information by extracting data from authoritative sources and all target resources both on-premises and in the cloud, then performing initial access certifications to clean up that data.

- **Data aggregation and correlation:** The aggregation and correlation process resolves the inconsistencies between the various sources of identity data, creating an enterprise-wide view that enables the organization to implement appropriate controls and better manage risk. This process provides visibility to accounts that do not correlate to users in authoritative sources (orphan accounts and system/service accounts) and enables removal of those accounts or assignment to owners for ongoing management.

- **Baseline access certification:** After data aggregation and correlation, the next step is to perform an initial "data cleanup" certification on the newly-centralized identity data. At this stage, data/application owners and people managers should review the access privileges for all users. These initial certifications should be used to establish a reliable baseline of data. It's not unusual for organizations performing a baseline certification to find that 10 to 25 percent of user access privileges are inaccurate or inappropriate and should be revoked. After revocations are performed, this cleansed data will be utilized by other identity management functions, including ongoing access certifications, policy enforcement, access requests and provisioning.

Step 2

Building a Governance Model

Now that you have a clearer picture of the current state of your data, and it is centrally visible, now you need to define the policy and controls the organization will use to ensure that all identity processes are performed in accordance with the organization's policies and risk management strategy. The governance model covers important components such as access policies, roles and risk.

- **Policy model:** As part of configuring the controls environment for identity governance, the organization will need to define the identity policies required to meet corporate and regulatory requirements across all critical resources. Identity policies that can be defined at this stage include separation-of-duty (SoD) rules that prevent users from holding potentially dangerous combinations of roles or entitlements, password policies and other access policies that can enforce rules such as "no user can hold more than one account on a resource."

- **Role model:** Roles are an important component of identity governance because they gather lower-level entitlements into like-minded groups, making it easier for business staff to review and approve user access privileges. The process of creating roles can be pursued incrementally based on the organization's needs; many enterprises begin by focusing on a defined set of departments or applications based on compliance or other business drivers. Once roles have been defined, they can be leveraged by many components of identity governance, including access certifications, policy enforcement and access request management.

- **Risk model:** An identity risk model can be used to strengthen detective and preventive controls – access certifications, access approvals or even authentication factors – for high-risk users and applications. For example, a person with simple read-only privileges and no access to critical applications would likely be considered low-risk, while a person who has numerous policy violations and has not been certified recently or has access to key applications would be considered high-risk.

Step 3

Automating Detective Controls

Once the organization has established a baseline of accurate identity data and built key components of the governance model, it's time to focus on automating and streamlining your processes for detective controls. This phase consists of two major components:

- **Access certifications:** Access certifications make it easy to perform regularly scheduled access reviews by application or data owners, people managers or a combination of both – or to review user access based on detected events, such as a position or manager change. Building on the policy, role and risk models already established, these reviews clearly highlight detected roles, policy violations and any changes from the previous certification (new users, new roles or new entitlements). This information enables reviewers to quickly focus on areas of potential risk and make better decisions.

- **Policy violation detection and remediation:** After the policy model is defined, the organization can automatically scan and analyze identity data to quickly detect any issues, such as SoD violations. Based on these scans, detailed reports can be generated, showing violations grouped by application, department or geography. In addition, organizations can customize how policy violations are handled once they are detected. For example, low-severity violations can be summarized in reports, whereas high-severity alerts can automatically trigger notifications to managers for immediate remediation.

Step 4

Embedding Preventive Controls in User Lifecycle Processes

Many organizations make the mistake of focusing their compliance efforts too heavily on detective controls: finding areas of non-compliance (after the fact) and fixing them. What organizations need is a balance of detective and preventive controls. Preventive controls will help to ensure that compliance violations are not reintroduced into the environment, enabling organizations to not only get compliant, but stay compliant. Areas of user lifecycle management that should incorporate preventive controls include:

- **Self-service access request:** Centralized access request management allows managers and end users to conveniently request new access or make changes to existing access privileges within the constraints of pre-defined identity policy and role models. As a further preventive control, flexible approval workflow can be configured to ensure manager, application owner or other approvals are pre-emptively granted before access is even requested, reducing the time it takes to provision access to a new, approved application.

- **Password management:** To ensure strong, secure passwords are in use, the organization should define password policies for all applications. This will enable the organization to enforce regular password changes, in addition to ensuring password strength and history policies are met when passwords are changed.

- **Event-based lifecycle management:** To certify that access changes such as employee terminations are handled quickly and accurately, organizations should implement automated provisioning based on triggers from authoritative feeds. By applying predefined policy to all provisioning processes, organizations can ensure users acquire only the most appropriate levels of access for their job function.

Step 5

Performing Closed-Loop Validation

The final step in deploying identity governance involves the fulfillment of access changes on target resources such as applications, databases and systems. In other words, this phase of the project is focused on ensuring that all changes triggered by revocations, access requests or lifecycle events are successfully implemented within the IT environment.

Closed-loop validation of all access changes involves three steps that can be performed as part of routine operations:

- **Periodic data aggregation:** Data aggregation should be scheduled to automatically run on a regular basis to ensure that all access changes required during access certifications or for policy conformance have been made.

- **Exception notification:** As an output of closed-loop validation, you should report all exceptions, such as access privileges that were revoked during a certification but have not been removed from a resource. This will enable prompt removal of those accounts or assignment to owners for ongoing management.

- **Proof of compliance:** As a final step in the compliance process, it's important to generate audit reports on the data aggregated from each resource and validate the access privileges that were revoked during a certification process or policy violations that were remediated.

Conclusion

SailPoint Can Help Your Organization Get Compliant and Stay Compliant

SailPoint solutions are specifically designed to help organizations better manage risk and meet the identity governance compliance requirements of government and industry regulations. Using a business-friendly approach to translate complex identity data into understandable information, SailPoint empowers business users to collaborate and assist IT staff in compliance and governance processes.

With SailPoint, you can automate the entire access certification process, establishing repeatable practices for more consistent, reliable and easier-to-manage access reviews. You can save significant time and money over manual methods (e.g., spreadsheets and email) with a streamlined solution that manages schedules, distributes access reviews to the appropriate personnel and tracks reviewer progress. And by automating the revocation of inappropriate access rights, you can quickly remediate access risks when detected. SailPoint also proactively detects violations already present in your environment. Once policies are defined, SailPoint solutions automatically enforce the policy, including entitlement and role separation-of-duty policies, application/account-based policies, activity policies and more.

To ensure your organization stays compliant, SailPoint builds preventive controls into all critical identity business processes, including all provisioning and user lifecycle management activities. SailPoint embeds policy checking and approval workflows in all lifecycle management and provisioning processes. And SailPoint's password management capabilities allow your organization to establish consistent, strong password policies to better protect corporate assets.

How SailPoint Solutions Automate Best-Practice Controls

COMPLIANCE REQUIREMENTS	RELEVANT SAILPOINT SOLUTIONS CHARACTERISTICS
Maintain comprehensive list of personnel with authorized access to critical, high-risk or sensitive resources	• Provides complete visibility into employees, contractors, partners and others with access to applications, systems and data, both on-premises and in the cloud • Provides extensive, on-demand reporting capabilities for compliance and audit purposes
Conduct reviews or certifications of user access to all high-risk applications	• Automates access review/certification processes across users and applications • Provides visibility to inappropriate or excess access • Automates revocation of access privileges
Detect and remediate access policy violations	• Centrally defines and enforces policies across all critical application environments • Automatically scans and analyzes identity data to uncover policy violations, then alerts based on severity • Provides detailed reporting on detected violations

Minimize and manage the scope and use of administrator, shared and privileged accounts	• Tracks and manages shared, service and privileged accounts • Enables the periodic review and approval of administrator, shared and privileged accounts by designated owners • Tracks and reports on the number of these types of accounts by application/system
Enforce preventive controls during provisioning processes (adding, changing, removing access)	• Requires manager or administrator approval for access changes • Enforces policy at the point of request • Prevents new violations by evaluating any proposed changes to user access against policies • Detects and alerts on events that violate policies
Define and enforce password policies for users and administrators on all systems	• Provides consistent enforcement of password policies including change frequency and minimum/maximum length and history • Provides an easy-to-use interface for resetting or changing passwords immediately and according to policy
Provide closed-loop validation of all access changes	• Provides complete visibility into status of all revocations and remediated policy violations – detecting rogue access or failure to remove • Provides proof of compliance based on data aggregated across all high-risk resources
Provide reporting and analysis tools to track and measure compliance	• Provides reports for critical compliance-related activities • Reports on key metrics via our user-friendly dashboard with at-a-glance charts, graphs, detailed reports and drill downs to source data • Provides ad hoc query capabilities to search and analyze identity data across the enterprise

**SAILPOINT:
THE POWER
OF IDENTITY™**

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in virtually every industry, including: 9 of the top banks, 7 of the top retail brands, 6 of the top healthcare providers, 6 of the top property and casualty insurance providers, and 6 of the top pharmaceutical companies.