SailPoint

eBook

A how-to guide: Identity security & compliance

Achieve continuous compliance with an AI-driven approach

FISMA GDPR HIPAA ISO NIS2 NIST PCI DSS SOX

Preface

In today's digital era, identity security has emerged as a pivotal factor in an organization's ability to meet compliance requirements, shaping enterprise security and trust. Identity security goes beyond mere adherence to regulations; rather, it provides a strategic, proactive approach to compliance by ensuring the security of all identities and their access. Identity security enables organizations to govern access, track usage, and enforce policies for all users, apps, and data to automate regulatory enforcement efforts and demonstrate compliance in the face of ever-changing regulations.

If you struggle to effectively implement compliance processes and integrate them into your systems and infrastructure, a modern identity security solution that leverages AI is the launching pad you need to improve effectiveness and reduce the costs of sustainable, continuous compliance.

Let's explore the evolving dynamics of compliance and identity security, revealing their impact on building trust, lowering risks and costs, driving business strategy, and navigating the complexities of the digital age.

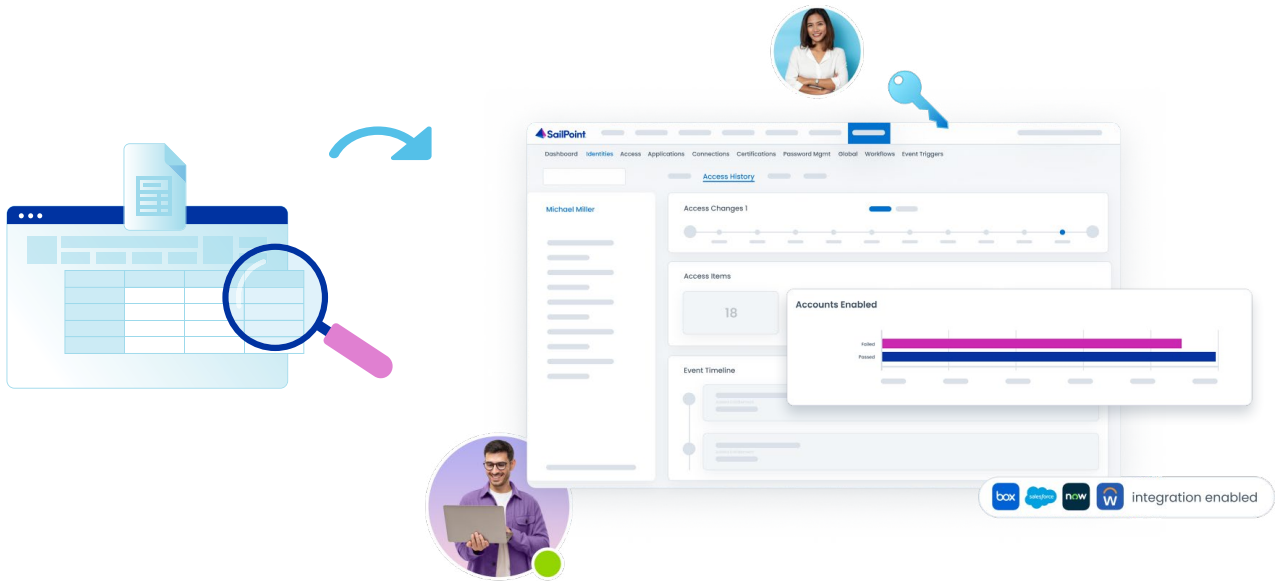
From manual to automated: Transforming compliance

Compliance can be complex and difficult — and as a result, costly. Meeting industry and regulatory mandates requires organizations to regularly review and certify user access. This leaves many constantly battling with error-prone and inefficient processes such as manually generating access reports, rubber stamping access approvals, and manually remediating inappropriate user access privileges.

If you find your organization struggling with any of the following, then it may be time to simplify your compliance processes.

- Building or leveraging multiple, homegrown solutions to handle audit and compliance needs
- Hiring full-time staff or consultants to handle compliance projects like access certifications and separation-of-duty (SoD) policy enforcement
- Requiring application owners to manually export and then format data for the next audit
- Using inefficient tools like spreadsheets and email to drive manual compliance processes
- Treating high-risk and low-risk users the same, where insufficient attention is given to high-risk users, or spending too much time and effort on low-risk users

To gain better control of your identity data, you need to replace expensive, error prone paper-based manual processes with centrally defined policies and automated access certification processes. By doing so, not only can you significantly reduce the cost of compliance, but you can also establish repeatable practices for a more consistent, auditable, reliable, efficient, and easier-to-manage access certification effort.



4 steps to simplify compliance processes

If audit deficiencies and the high cost of compliance are top of mind issues in your organization, then you may want to focus on compliance automation initially. You may already be in the process of establishing a "least privileged access model" as required by many regulatory frameworks. Least privilege is also a key element of enforcing a zero trust approach to identity security. With least privilege you ensure that people only have the access they need to perform their job function so that if an identity or an account is breached, the exposure of such a breach is limited to the access that person was supposed to have, rather than over-privileged access users frequently have, which could lead to higher fines and more exposure.

The journey to establish a robust compliance framework begins with four foundational steps designed to enhance visibility, security, and efficiency within your organization. By implementing these strategies, companies can create a solid baseline for managing compliance effectively, leveraging AI to streamline processes and mitigate risks.

1. Gain centralized visibility

The starting point for any compliance project should be to understand the current state of users by getting a central view of identity access across the organization. This stage involves creating a single repository for user and access information by integrating with and aggregating data from your authoritative sources, such as HR systems and contractor databases, and target resources.

2. Identify and close all orphan accounts

Finding and eliminating orphan accounts is one of the most effective risk mitigation steps you can take in your compliance project. Once you've identified these high-risk accounts, you can launch remediation actions for all unowned accounts — remove, mark as service, or, where possible, correlate to known identities.

3. Detect and remediate outliers

The next step in the data clean-up process is to identify outliers: users that have significantly different access from what is expected. As you build the business case for your identity security program, look for a solution with AI which can spot risky users and access outliers and significantly strengthen security by helping to detect and remediate vulnerabilities.

4. Automate access certifications

Next, generate a certification campaign that can help automate access reviews for all users. Today, your team can be assisted by recommendations fueled by AI which simplify and shorten the certification review cycle. Your team will easily know whether or not it is safe to approve or deny access. Initial certifications should be used to establish a reliable baseline of data.

With the groundwork laid for adopting compliance best practices, it's crucial to understand the regulatory landscape that shapes these requirements.

Protecting data across industries

Navigating the landscape of compliance regulations is essential for organizations across various industries, especially those in highly regulated sectors such as financial services, healthcare, government, and manufacturing. Regulations are designed not only to protect sensitive information and maintain privacy but also to uphold the integrity and trust of businesses in the digital age.

Here's a closer look at some of the most common compliance regulations:

National Institute of Standards and Technology (NIST) Cybersecurity Framework: Offers guidelines for improving cybersecurity across critical infrastructure in the U.S., widely utilized by various organizations to manage cyber risks effectively.

Network and Information Systems 2 Directive (NIS2): Expands the original EU NIS Directive, strengthening cybersecurity resilience across essential services (energy, transport, banking, health) and digital service providers (cloud services, search engines, online marketplaces).

General Data Protection Regulation (GDPR): A pivotal regulation within the EU that sets the standard for data protection and privacy, affecting companies worldwide that deal with EU citizens' data.

Health Insurance Portability and Accountability Act (HIPAA): Governs the protection of sensitive patient health information in the United States, critical for healthcare providers and their associates.

Sarbanes-Oxley Act (SOX): Imposes strict auditing and financial regulations on corporations in the United States to protect shareholders and the general public from accounting errors and fraudulent practices.

Payment Card Industry Data Security Standard (PCI DSS): Essential for any organization handling credit card transactions, requiring them to maintain a secure environment for cardholder data.

Federal Information Security Management Act (FISMA): Affects U.S. federal agencies, mandating the protection of information systems against threats.

International Organization for Standardization (ISO) 27001: Provides a framework for information security management systems (ISMS), applicable to organizations of any size.

Understanding and adhering to these regulations is foundational for securing organizational integrity and building trust with stakeholders, highlighting the necessity of a strategic approach to compliance and identity security.

How SailPoint can help

Leveraging artificial intelligence and machine learning, SailPoint's identity security solutions facilitate compliance by offering a comprehensive approach to managing and securing digital identities across your organization. Through automation of access reviews, role and policy management, and risk detection, SailPoint helps ensure adherence to global regulatory requirements by streamlining the process of granting, modifying, and revoking access rights – ultimately reducing the potential for access-related compliance violations. This proactive stance on identity security significantly aids organizations in maintaining a strong compliance posture in the face of evolving regulations and threats.

The benefits of our strategic approach to compliance and identity security are clear:

- **Streamlined Operations:** Automated workflows and intelligent decision-making processes lead to more efficient operations and a significant reduction in manual effort.
- **Enhanced Security Posture:** Continuous monitoring and adaptive policies contribute to a stronger defense against both external and internal threats.
- **Cost Savings:** By removing manually processed compliance tasks and automating identity practices, organizations can achieve a lower total cost of ownership and a faster time to value.

To fully understand how SailPoint can secure and streamline your compliance and identity security processes, schedule a consultation with a member of the SailPoint team. Experience the difference that a strategic approach to compliance can make for your organization.

Visit **sailpoint.com/solutions/maintain-compliance** to learn more.

SailPoint

About SailPoint

SailPoint equips the modern enterprise to effortlessly manage and secure access to applications and data through the lens of identity - at speed and scale. As the category creator, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency. SailPoint helps the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.