Deloitte. | SailPoint

JUMPSTART YOUR IDENTITY SECURITY PROGRAM:
10 ACTIONS FOR REAL-TIME IMPACT

Why identity security can't wait

Security breaches can result in financial loss, reputational damage, and regulatory exposure—costs no organization can afford. Today, a strong identity security program does more than help defend against threats: it helps organizations align with compliance requirements, simplifies access for legitimate users, and anchors the shift to Zero Trust architecture.

Yet many organizations are still navigating inconsistent identity practices and fragmented controls. As digital ecosystems rapidly expand, so does identity related risk. Proactive governance has become not just a best practice but a business imperative—essential for resilience, trust, and competitive advantage.

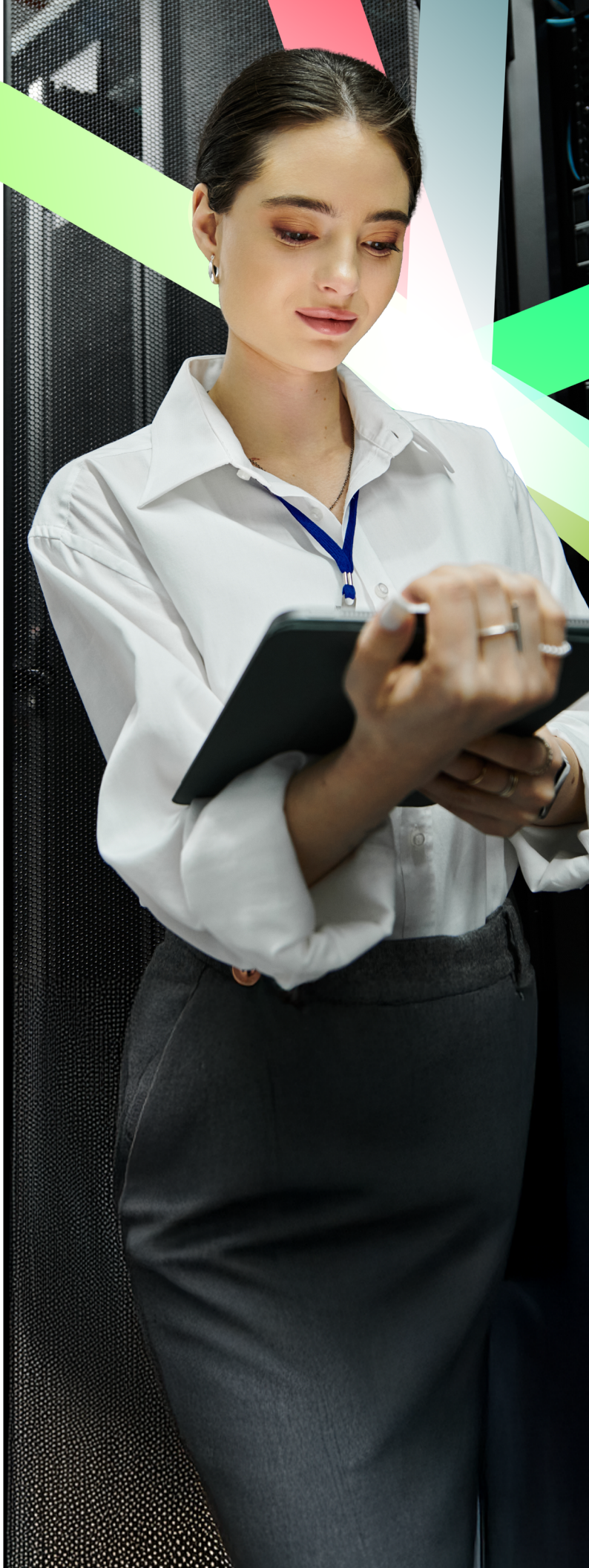
The impact of strong identity security

Identity security isn't just about protection; it acts as a catalyst for driving business outcomes. When thoughtfully executed, identity programs generate measurable advantages that stretch across both operations and strategy.

Organizations leading in identity security consistently balance four key objectives:

- **Productivity + User Experience**
- **Risk + Cost and complexity**

By integrating these objectives, top performing programs transform security investments into real business value. The following 10 practical, quick-win actions offer a way for identity leaders to build momentum, demonstrate value early, and strengthen the foundation of their identity security initiatives.



10 high-impact actions to build momentum

Driving rapid progress in identity security requires focusing on actions that deliver clear value early. By targeting quick, high-impact wins—aligned with productivity, user experience, cost, and risk—identity leaders can quickly demonstrate program momentum, secure stakeholder buy-in, and lay the groundwork for long-term success.

1 PRIORITIZE AND ONBOARD HIGH-IMPACT APPLICATIONS (RISK AND/OR VOLUME)

Start by identifying and prioritizing applications that are both high-risk and mission-critical. Early onboarding of these systems can deliver measurable improvements in access oversight and help quickly demonstrate the value of your identity program.

> **Why it matters:**
> Focusing early efforts where risk and business value are greatest improves visibility, control, and stakeholder confidence.

2 IMPLEMENT SEGREGATION OF DUTIES (SOD) CONTROLS

Focus initial SoD efforts on areas like finance, HR, procurement or administration, where overlapping access could present real business or compliance risks. Demonstrating prevention of critical access conflicts elevates governance assurance.

> **Why it matters:**
> Addressing the most impactful access conflicts up front can help strengthen governance and prevent compliance issues.

3 STRENGTHEN DEPROVISIONING COVERAGE AND VALIDATION

Review and verify existing leaver processes to ensure consistent enforcement across applications. Closing automation gaps and validating end-to-end disablement reduces orphaned accounts and provides stronger evidence of complete deprovisioning.

> **Why it matters:**
> Reducing gaps and validating disablement can lower risk and improve audit readiness.

4 INTRODUCE INACTIVITY-BASED DISABLEMENT

Identify and disable accounts that are inactive, while maintaining exceptions for service or emergency access. Cleaning up unused accounts reduces exposure and results in cleaner user inventories.

> **Why it matters:**
> Disabling dormant accounts limits lingering risks and improves system hygiene.

5 IMPROVE DATA QUALITY AND INTEGRITY ACROSS IDENTITY SOURCES

Evaluate the key data flows between HR, directories, and target systems to identify inaccuracies and clarify ownership for corrections. Improved data quality leads to fewer manual fixes, faster fulfillment and greater trust in identity data.

> **Why it matters:**
> Strong data integrity streamlines automation, reduces provisioning errors, and supports trust in identity systems.

6 CREATE A REUSABLE ONBOARDING KIT

Develop standardized templates, configuration patterns, and testing guidelines to make onboarding repeatable and efficient. This supports faster onboarding cycles and predictable integration outcomes.

> **Why it matters:**
> Standardized onboarding accelerates future integrations and maintains consistent quality.

7 INTRODUCE ATTRIBUTE-BASED ACCESS RULES

Pilot simple, rule-based logic that automatically grants or revokes access based on user attributes like department, role type, or region. This enhances automation and minimizes reliance on manual provisioning.

> **Why it matters:**
> Rule-based automation helps scale access control and reduces manual workload.

8 RUN RISK-FOCUSED CERTIFICATIONS FOR ONBOARDED APPLICATIONS

Target review campaigns around high-risk or privileged access, reducing unnecessary noise and reviewer fatigue. Streamlined campaigns may yield higher-quality decisions and emphasize true risk.

> **Why it matters:**
> Targeted certifications focus review effort, create actionable results, and emphasize what matters most.

9 DEFINE ENTITLEMENT STANDARDS AND CLEAN UP NOISE

Establish clear policies for entitlements, including naming conventions, descriptions, owners, and risk classifications. Use these standards to clean up redundancies and inconsistencies, supporting both automation and business reviews.

> **Why it matters:**
> Defining standards creates a cleaner, more usable catalog for automation and review.

10 PUBLISH A ONE-PAGE EXECUTIVE DASHBOARD

Develop a concise, visual dashboard highlighting progress in onboarding, certifications and automation. Communicating success with concrete data enables continued visibility and financial support for your program.

> **Why it matters:**
> Sustained leadership engagement and program funding depend on clear, tangible results.

Delivering real, lasting results from your identity program isn't just about the technical wins, it's about making change stick across your organization. The following components can help transform high-impact actions into long-term value:

- Organizational change management to guide adoption and foster culture shift.
- Effective program management to align resources, track progress, and clear obstacles.
- Detailed project plans to drive focus, accountability, and steady milestones.

Defining your North Star
A compelling vision—your "North Star"—helps unify teams, clarify priorities, and anchor every initiative to business goals. Setting this vision involves not just clear technical outcomes, but also establishing strong team structures and engaging the right stakeholders from the outset.

By combining practical, high-impact actions with these foundational practices, you can be better positioned to maximize adoption, sustain momentum, and position your identity security program for measurable, enduring success.

How Deloitte and SailPoint collaborate to accelerate transformation

Deloitte and SailPoint form a powerful alliance, helping organizations modernize and secure their identity landscapes.

Deloitte brings deep advisory experience, demonstrated implementation services, accelerators, and strong change enablement to help facilitate program delivery and user adoption.

SailPoint delivers a leading-edge identity platform, empowering organizations with advanced controls, analytics and automation for robust, scalable identity security.

By joining forces, we deliver:

- Automated identity lifecycle management: Streamlining the process of granting, modifying and removing access as people join, move or leave.
- AI-driven identity analytics: Leveraging machine learning to detect unusual access patterns, predict risks, and determine compliance.
- Integrated audit and compliance controls: Simplifying policy enforcement and enabling efficient, transparent reporting for regulators and internal stakeholders.

Together, our collaboration enables clients to:

- Adopt a risk-based, preventative approach to identity security—balancing protection with a seamless user experience
- Reduce certification fatigue and repetitive manual reviews by targeting what matters most.
- Continuously improve identity operations, keeping pace with evolving regulatory requirements and business growth.

Begin your journey with an identity security maturity assessment

As your first step in developing a plan for improving your identity security program, you can complete the SailPoint online identity security maturity assessment[1]. Going through this process can help you understand which identity security horizon your company has reached and how you can move forward confidently.

If you have questions about deploying a security identity solution, SailPoint welcomes the opportunity to assist. **Contact us today for more information**.

[1] **SailPoint Assessment web page**