Deloitte. SailPoint

ACCELERATING A *CERTIFICATION-FREE FUTURE*

September 2025

Accelerating a certification-free future

As digital ecosystems expand, organizations face increasing challenges in ensuring that their people have the right access to sensitive applications, data, and systems. Traditional access certifications—designed for security and compliance—create a burden. Reviewers are presented with ambiguous data characterized by lack of clear information and excessive manual processes. A mandate to "just get it done", invites risky trade-offs that often lead to rubber-stamping certifications.

Symptoms of a broken identity system

Access certifications were meant to verify appropriate access and demonstrate compliance. Instead, they've become overused, misunderstood, and ineffective—generating massive review lists that business users don't understand, don't value, and don't have time to assess. The result? Rubber-stamping—not from negligence, but overhead and fatigue.

But rubber-stamping is just a symptom. The real issue is a certification process that's too frequent, too risk-agnostic, and too manual. The solution isn't to enforce certification rigor—it's to rethink the whole approach. That means questioning the status quo, understanding what is being reviewed, why and when, and then reshaping certifications with a risk lens. Certification doesn't just need streamlining—it needs transformation.

The real cost of broken certifications:

$4.44M AVERAGE COST

to recover from a cyberattack with over-provisioned access often cited as a contributing factor[1]

55% OF INSIDER INCIDENTS

involve employee negligence, often including behaviors like bypassing policies or rubber-stamping access certifications[2]

75% OF SECURITY FAILURES

by 2023 that will result from inadequate management of identities, access, and privileges[3]

We believe the solution lies in an approach that not only simplifies certifications but accelerates the path to eliminating them altogether. While most organizations aren't ready to completely eliminate certifications today, our approach begins by making certifications smarter, lighter, and more targeted—then reducing their frequency and scope over time as provisioning and deprovisioning processes mature—paving the way for a certification less future.

The potential benefits of the Deloitte-SailPoint risk-based approach for access certifications

1 IMPROVED SECURITY

Reduces the risk of each user by implementing a more rigorous access certification program.

2 OPERATION EFFICIENCY

Decreases human resource hours while increasing the speed of access certification delivery.

3 REGULATORY COMPLIANCE ALIGNMENT

Helps assessors and auditors understand the risk- based approach the organization takes to manage and ensure access is appropriate.

4 ENHANCED USER EXPERIENCE

Prevents rubber stamping while increasing certification program effectiveness.

5 INCREASED RESOURCE PRODUCTIVITY

Tightens integration between security and the business.

1. IBM. Cost of a Data Breach Report 2025. 2025.
2. Ponemon Institute. The Security Risk Organizations Should Not Ignore: Careless, Negligent and Malicious Insiders. 2025.
3. Gartner. Best Practices for Optimizing IGA Access Certification. 2022.

Engineering the end of certification fatigue

Deloitte and SailPoint are uniquely positioned to help solve the access certification problem—not by repackaging the same process with new tools, but by reimagining how access is governed in the first place.

Our model can help reduce the burden on business and IT teams by focusing on three practical controls that reduce the need for certifications:

- Intelligent provisioning
- Timely deprovisioning
- Purposeful certifications (only when needed)

These map directly to the identity governance foundation—provisioning, deprovisioning, and certification—a model strengthening with automation, policy logic, and context-aware decisioning.

By embedding preventive and detective controls into every access decision, our joint solution is designed to shift reviews away from volume-based processes toward precision-driven oversight—reducing effort without compromising security.

The three-legged stool of access governance

At the core of any secure and efficient identity program are three interdependent components: provisioning, deprovisioning, and access certifications. These form the three-legged stool of access governance. When one leg weakens, the integrity of identity security falters

Provisioning and **deprovisioning** are preventive controls—they manage access proactively, helping to ensure that the right people have access only when they need it, and that access is revoked immediately when it's no longer appropriate.

Access certifications, by contrast, are detective controls—a fallback mechanism used to verify that access remains appropriate over time.

The more effective and intelligent your provisioning and deprovisioning processes become, the less you need to rely on certifications. This enables organizations to shift from frequent, manual reviews to more targeted, risk-based certifications—eventually reducing them to only high-risk or exceptional cases.

By modernizing all three components, organizations can build a scalable and secure identity program—while reducing the volume and burden of certifications over time. While certifications still play a role in most organizations today, our approach treats them as a temporary safety net—not a permanent fixture. By strengthening provisioning and deprovisioning and layering in smarter automation, we help organizations phase out broad certifications in favor of precision access governance. Over time, the need for manual certifications shrinks—until only rare or high-risk access scenarios remain. In some mature environments, that number may realistically approach zero, especially when combined with AI capabilities and a robust role-based access approach.

Prioritization where it matters most

Four levers for simplifying and reducing access certifications.

Many organizations certify access using massive lists of entitlement data with little risk context—overwhelming reviewers and increasing the chance of errors. Our approach uses four complementary levers to shrink certification scope, highlight high-risk access, and eliminate reviews that don't add value.

Entitlement Clarity: The prerequisite to smart certifications

A critical enabler of this approach is ensuring that entitlement data includes clear, relevant business context – such as what the access allows, and who owns it. Without this foundational clarity, even the best filtering mechanisms fall short.

This is a heavy lift, and organizations need more than theory. SailPoint has the capability to enrich entitlement data using AI and peer-based modeling—even pulling information from external sources to enhance context. Deloitte brings its own library of industry-standard entitlements, along with the regulatory and domain experience to align access data with real-world risk.

While many organizations struggle to reach this level of entitlement maturity, progress can start with small wins: assigning ownership, adding descriptions, and classifying access types to build momentum over time.

Lever 1: Eliminate low-value access from review

Use risk-based filters and entitlement metadata to remove noise from certifications. Placeholder entitlements, empty roles, and lower-environment artifacts should never hit a business reviewer's screen. Likewise, access tagged as low risk can often be excluded entirely from manual review. By applying contextual logic and tiered sensitivity levels, organizations can cut review volume dramatically while focusing on what matters.

Deloitte, with its deep industry and regulatory experience, helps organizations apply a practical risk lens to entitlement data—enabling more precise scoping and helping determine what truly needs review.

Applies to: Certification - Detective

Lever 2: Standardize access with RBAC

Mature Role-Based Access Control (RBAC) reduces review scope by bundling common access into approved roles. When most of a team's access is pre-approved and assigned through roles, only exceptions require certification—lowering fatigue and improving review quality.

Applies to: Provisioning - Preventive

Lever 3: Apply Modern IAM controls

With the Use preventive controls like:

- Just-in-time access
- Dynamic SoD enforcement
- Policy-driven approvals
- Automated removal based on inactivity or last login

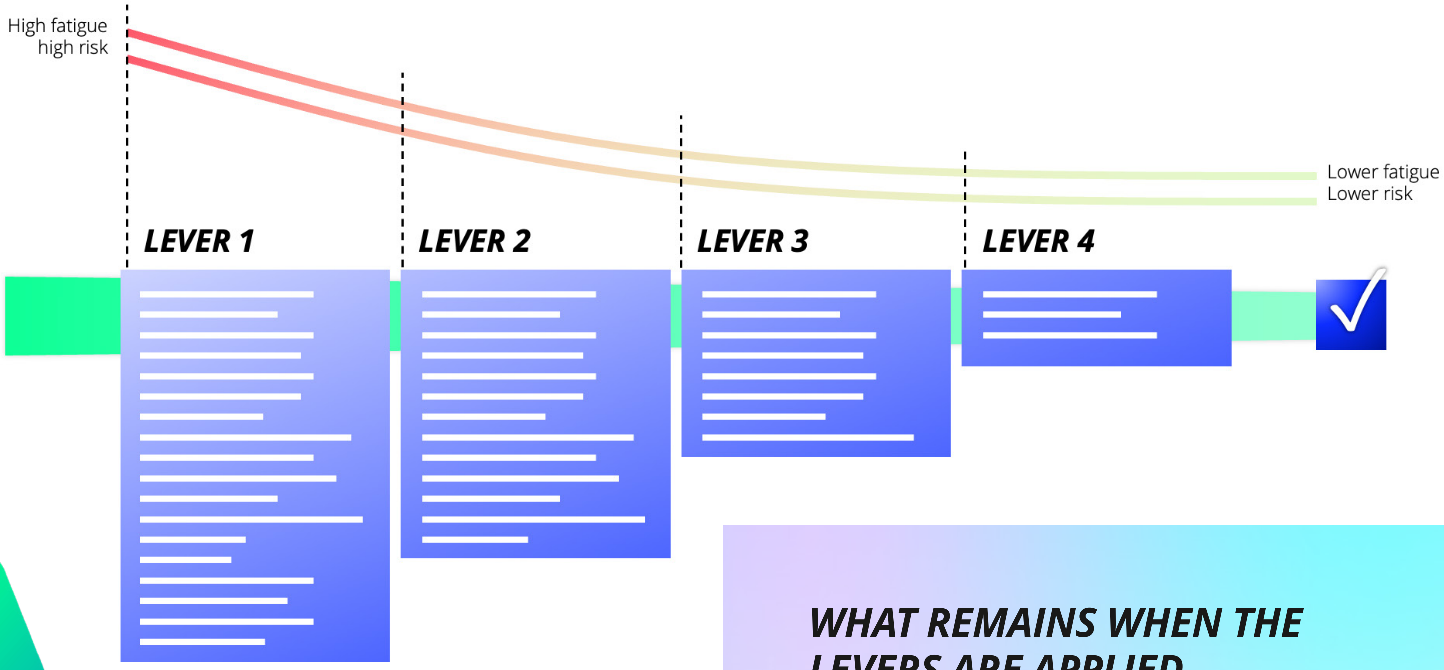
These block risky access before it's granted—or remove it when no longer needed—reducing what even needs to be reviewed in the first place.

Applies to: Provisioning, Deprovisioning - Preventive

Lever 4: Certify only what changed

Focus certifications only on access that changed since the last cycle—including new entitlements, changed roles, or user attribute shifts. This dramatically shrinks the scope and highlights what truly requires attention.

Applies to: Certification - Detective



WHAT REMAINS WHEN THE LEVERS ARE APPLIED

When organizations apply these four levers, what remains is a sharply reduced, high value access that genuinely requires human review.

This approach helps organizations focus only on what matters, minimizing the certification burden while improving quality and audit confidence.

How AI can help further reduce the need for certifications

No matter the frequency or volume of certifications, access reviewers still need better context on the users and entitlements being reviewed. That's where AI shifts the game—delivering decisions at scale, driven by data, not guesswork. AI provides the user with contextual information that simplifies and improves decision making.

By combining Deloitte's risk-based methodology with SailPoint's embedded AI services, organizations can reduce review volume, accelerate response times, and improve accuracy—while setting the foundation for a certification-free future.

What Deloitte + SailPoint AI enables

REDUCE ACCESS RISK

- Detect risky or anomalous access with peer-based analysis
- Flag outliers before they become incidents
- Minimize standing access through dynamic modeling

CUT REVIEW VOLUME

- Certify only what changed via delta detection
- Enhance meta data and filter out low-risk entitlements using AI-powered risk scoring
- Adjust review cycles dynamically based on access sensitivity

IMPROVE DECISION ACCURACY

- Recommend access based on peer and role analysis
- Suggest approve/revoke actions during certification
- Auto-discover role groupings based on access behavior

These aren't just automations—they're strategic enablers. AI helps identity programs evolve from reactive oversight to real-time intelligence. As these capabilities mature, they don't just reduce certification effort—they render it obsolete.

WHERE AI MAKES THE BIGGEST IMPACT

Reduces review fatigue across business and IT

Flags risky access that manual processes miss

Boosts decision accuracy with peer-based analysis

Accelerates onboarding and reduces time-to-productivity

Enhances audit readiness and response speed

Enables true risk-based governance at scale

RECLAIM CONTROL.
REDUCE EFFORT.

Paving the way for a certification free future

Access certifications were never meant to carry the full weight of identity governance—yet that's exactly what many organizations have asked them to do. The potential result? Bloated reviews, business fatigue, and rubber-stamping at scale.

Deloitte and SailPoint can offer a solution. Not by tweaking the old process—but by replacing it with smarter provisioning, real-time access controls, and embedded AI that does the heavy lifting. Together, we help you shift from reactive oversight to proactive governance.

We've seen the data. The cost of inaction isn't hypothetical—it's millions lost, controls bypassed, and risks left unchecked.

If your certification process still looks the same (or worse) as it did five years ago, it's not just inefficient—it's exposing you. It's time to stop treating certifications as a compliance checkbox and start treating them as a failure to govern access correctly.

LEARN MORE:

Amit Chhikara
Principal
Deloitte & Touche LLP
achhikara@deloitte.com

Chris Gossett
Senior Vice President, Technology Services
SailPoint
chris.gossett@sailpoint.com

Stefan Paul
Senior Manager
Deloitte & Touche LLP
stepaul@deloitte.com

REDEFINE WHAT GOVERNANCE LOOKS LIKE

Because the future of identity isn't certified, it's engineered.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society, and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 415,000 people worldwide make an impact that matters at www.deloitte.com.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.