2024 STATE OF IDENTITY SECURITY IN FINANCIAL SERVICES

REDUCING RISK AND INCREASING EFFICIENCIES

A Global Survey of Identity and Security Leaders

July
2024

dimensional research

Sponsored by SailPoint

Introduction

This report reviews a global survey conducted by Dimensional Research of more than 300 Identity and Access Management (IAM), IT security, and audit and compliance leaders focusing on the current state of identity security solutions, challenges financial services companies are facing in governing identities, meeting security requirements, and ensuring compliance. The research also captured the frequency of security breaches and audit report findings to identify current solution gaps and needed features.

Executive Summary

Financial services companies are managing tens of thousands of identities, which at scale can be challenging to quickly manage and secure access for employees as they join, transfer departments, or leave a company. 77% state these problems are exacerbated by a rapid influx of identities often caused by mergers and acquisitions. Acquired companies may lack visibility into all their identities' access and may delay, inadvertently overprovision, or under-provision access. Additionally, nearly 8 out of 10 of participating companies indicated that overprovisioning creates vulnerabilities that increase cybersecurity risk. And 74% stated that too many of the identity processes for onboarding, offboarding, and transfers require too many manual steps. Challenges are further complicated by the need to continuously manage third-party access, achieve compliance, and reduce cybersecurity risk. A lack of automation can also limit efficiency, increase risk, and drive costs.

Top identity security (also known as identity governance) objectives for the next 12 months are focused on better identity control, securing non-employees, and creating efficiencies through automation. The findings also revealed 93% find meeting compliance is challenging, with three of the top four compliance issues centered around lack of resources, manual processes, and large time commitments. This led to 64% revealing they had an audit finding over the last two years.

When asked what functionality is needed in identity security solutions, the top capabilities centered on efficiency and mitigating risk both for compliance and security. This perspective is reinforced by identity professionals stating current tools require too many manual processes, lack automation, and are missing critical security capabilities. These needs are likely driving the 98% who are seeing value in SaaS-based identity security solutions, which participants indicate drive efficiencies, lower costs, and have quicker timeframes for utilizing new functionality and controlling access from anywhere. As identity security encompasses governing access to both employees as well as third-party non-employees to ensure compliance and security, it is key that companies rely on solutions that can meet changing requirements while minimizing burdens on identity teams.

Key Findings

- Inadequate Identity Security Creates Compliance and Security Risk
  - Managing third-party identities, audit and compliance, and employee access delays were the top reported identity governance challenges
  - 93% report numerous challenges in achieving compliance
  - 77% reveal that a rapid influx of identities increases risk
  - 74% have time-wasting manual identity processes for staffing changes
  - 77% admit overprovisioning creates cyberattack vulnerabilities
  - 79% have strong concerns about overprovisioning to non-employees

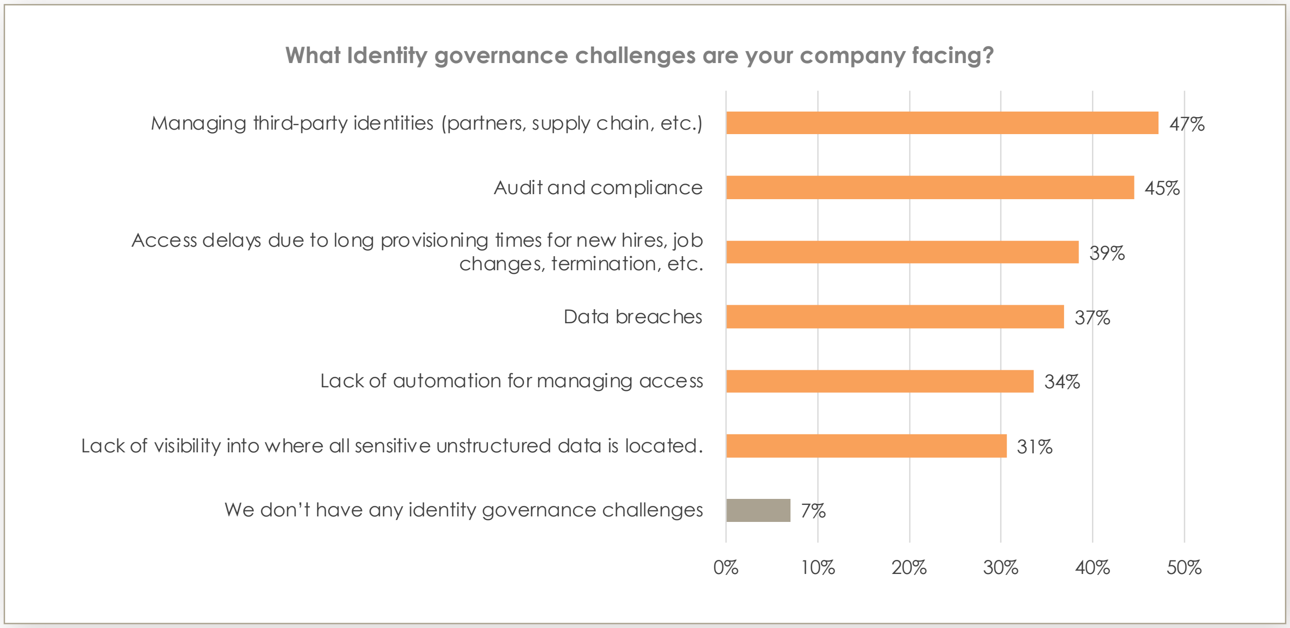
- Companies Set Identity Objectives to Improve Identity Governance Controls, Automation, and Secure Non-employee Access
  - 60% indicated that they want to improve identity governance controls (policies, certifications, etc.)
  - 48% wish to replace manual processes with automation
  - 47% reported a desire to expand their identity governance program to cover non-employees (contractors, partners, etc.)

- SaaS-Based Identity Security Solutions Provide Capabilities to Manage Risk as Identity Requirements Evolve
  - Top identity security needs center on risk management and efficiency, with increased productivity taking the top spot
  - Current tools lack efficiency, automation, and key security capabilities
  - 98% indicate key benefits from SaaS-based identity governance solutions

Detailed Findings

Most Companies Struggling with Identity Security Challenges

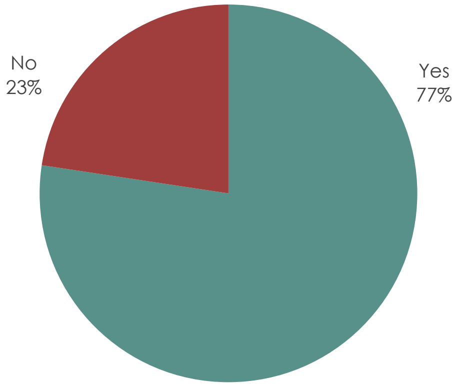
Financial institutions are managing a staggering number of identities that keep increasing. To understand the complications of managing many identities daily, identity and security leaders were asked about their top identity security challenges. At the top, representing the most difficult, is managing third-party identities (47%) which can be partners, suppliers, or services to support key financial processes such as credit checks, customer services solutions, stock trades, and more. Audit and compliance challenges placed next at 45%. Completing the top three challenges is access delays (39%) in provisioning or changes in employment status, such as a new hire or promotion. For financial institutions, IT systems and applications are critical to their business; and when employees can't access needed applications and data, the business is impacted. The fourth challenge is 37% who have concerns with data breaches which indicates breaches are in fact happening, and a lack of automation (34%). In short, only 7% of financial institutions surveyed don't have identity security challenges.



Mergers and Acquisitions Drive More Risk and Nearly Half Had Breaches

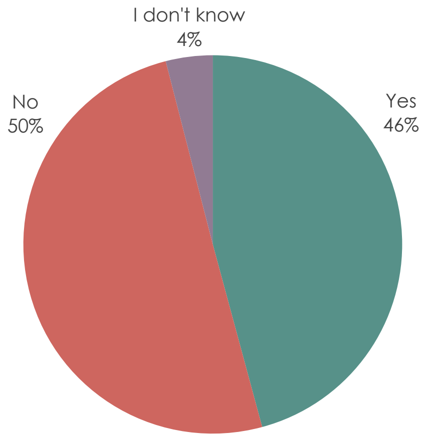
When the research sought to understand some of the key factors contributing to the identity challenges, 77% of identity and security experts stated that a rapid influx of identities from mergers and acquisitions (M&A) creates increased risk. The previously cited delays in access changes and lack of automation identity security challenges make M&As even more difficult.

At your company, do you feel that mergers and acquisitions create increased risk from an influx of identities?



Given the larger number of concerns about data breaches from the first chart in the report, the research sought to quantify the number of breaches a company has experienced. Unfortunately, 46% indicated they had a breach in just the last twenty-four months. The frequency of breaches indicates that identity security challenges create material risk that does impact the business. Also concerning are the 4% who don't know, which reveals a lack of communication and lessons learned to prevent further breaches.

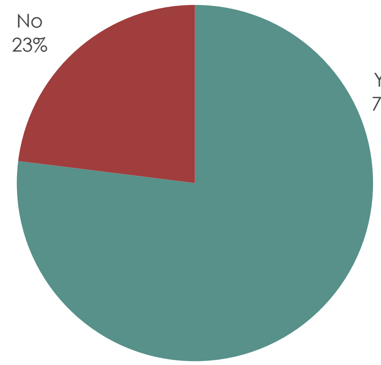
Has your company experienced a security breach over the last 24 months?



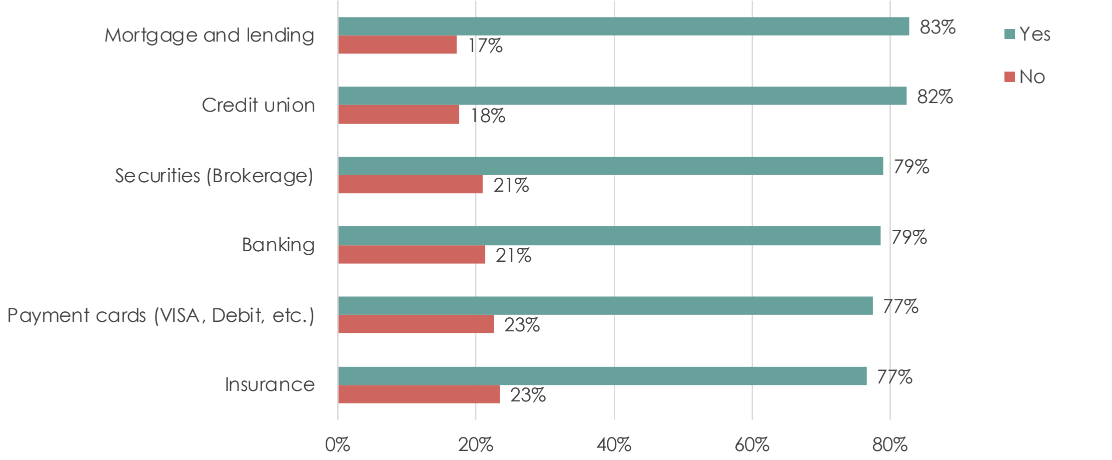
Overprovisioning Access Represents Tremendous Risk

One critical aspect of identity security is to prevent overprovisioning that would grant inappropriate access which can result in noncompliance, failure to meet separation of duties requirements, as well as providing access to Personally Identifiable Information (PII). But perhaps more concerning is the 77% of identity security professionals who stated overprovisioning access increases susceptibility to cyberattacks. Of the financial services industries, mortgage and lending led the financial services industry with 83% who noted increased cyberattack vulnerability resulting from overprovisioning. Just a few percentage points down is general banking at 79% and just a couple below that is insurance at 77% confirming a pervasive overprovisioning risk.

Do you think overprovisioned access leaves your company vulnerable to cyberattacks?



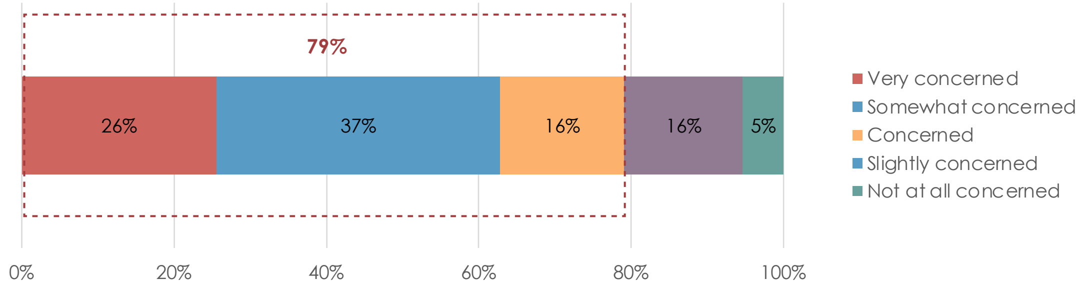
Do you think overprovisioned access leaves your company vulnerable to cyberattacks? (By Sub Industry)



High Concern for Overprovisioning Access to Third Parties

The key identity security challenges chart which led this report revealed that managing access to third parties or non-employees was a top problem. It is key to consider that non-employees can be anyone along a company's services value chain such as partners, suppliers, or contractors, as well as other systems that require access. When participants were specifically asked about risk associated with overprovisioning non-employees, 79% were concerned and over a quarter (26%) were highly concerned. Delving into the specific financial service areas, mortgage and lending again leads all with 84% concerned, banking just behind with 83% being concerned, and insurance with 77%.

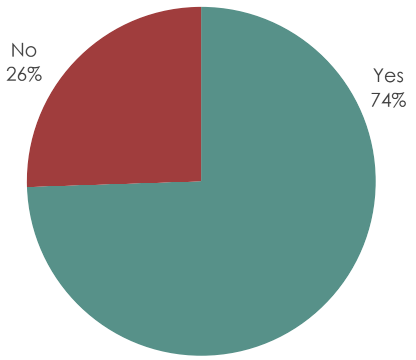
How concerned is your company about overprovisioned access risk to non-employees (contractors, partners, etc.)?



Manual Processes Slow Identity Changes and Updates

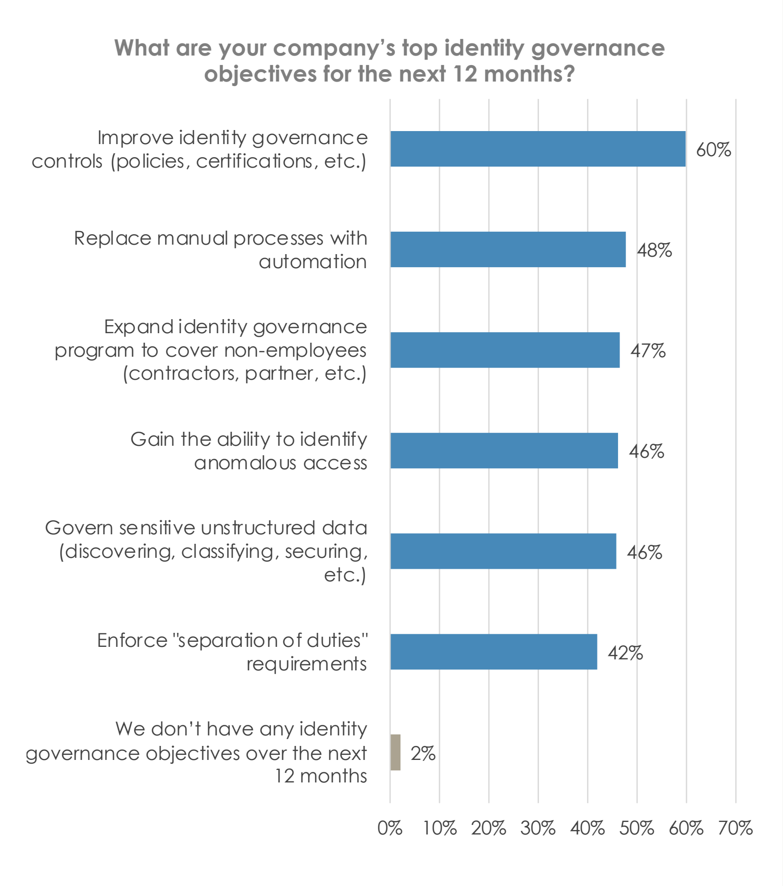
The third highest identity challenge reported was access delays, whether it be for onboarding new employees, changing roles, or revoking privileges for an employee who has left a company. One large contributor is that nearly three quarters (74%) of IAM and security leaders state their identity management processes require too many manual processes. Manual processes commonly add delays and provide an opportunity for mistakes, such as overprovisioning access. This finding reinforces the problem with large scale identity changes from M&A, and directly indicates a lack of automation.

Does your company have too many time-consuming manual identity processes for staffing changes (onboarding, offboarding, transfers, etc.)?



Top Objectives include Increased Identity Governance Control, Automation, and Securing Non-Employee Access

IAM and security leaders were asked to look forward and share what their identity security objectives are for the next twelve months. Taking the top spot at 60% is improving identity security controls (visibilities, enforcement, policies, etc.). The next five answers were nearly tied with only six percentage points separating them. Increasing the use of automation (48%) and directly including non-employees in their identity security strategies (47%) round out the top three. These objectives closely align to the top challenges, indicating an intent to resolve them. The next three identify anomalous access (46%), discover, and manage unstructured data (46%), and enforce separation of duties (42%), all look, in sum, to move their identity security toward a more proactive strategy to mitigate risk.



SailPoint's Perspective

Banking, payment card, insurance, credit union, and other sectors within the financial services industry are facing significant security, economic, and compliance challenges. As financial services institutions grow and transform, so too has their cyber risk. Mergers and acquisitions (M&A), rapid digital transformations, third-party risk, and increased amounts of unmanaged sensitive data have resulted in myriad and often high-profile data breaches.

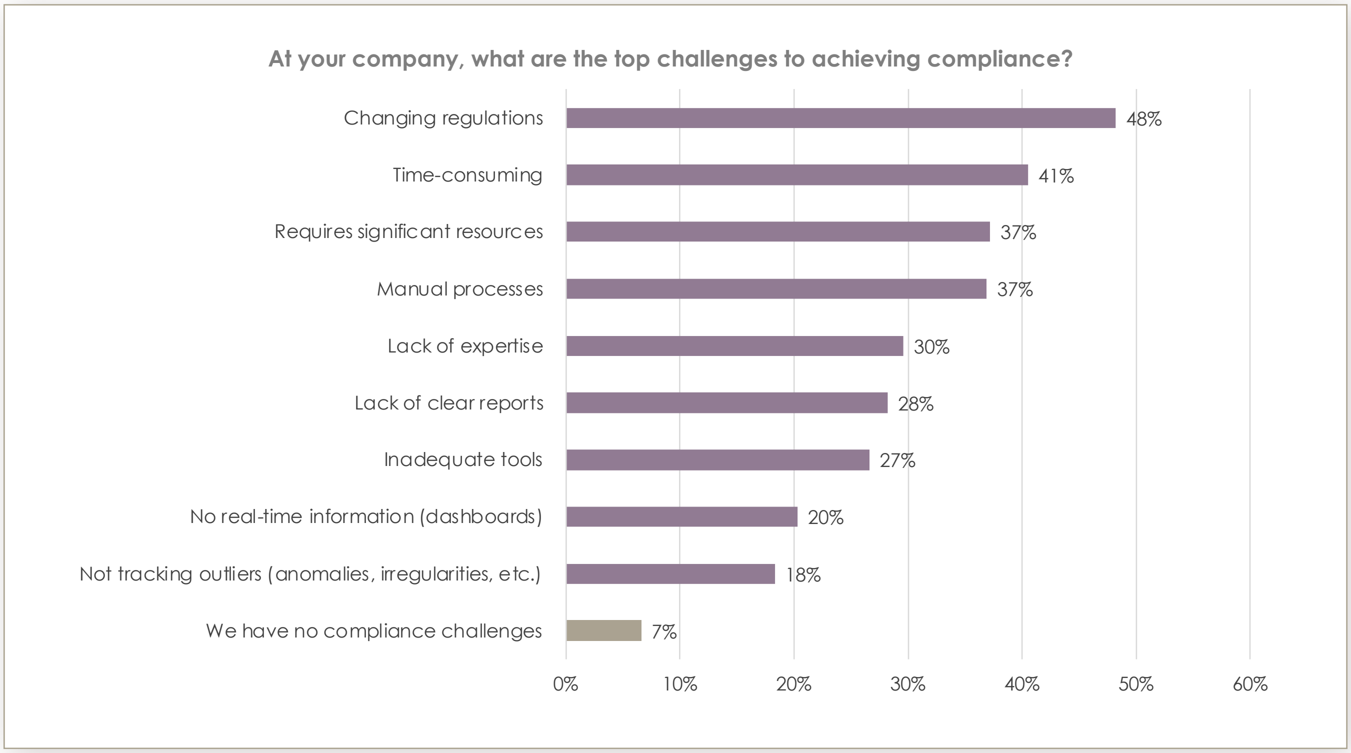
Financial institutions also need to reduce risks and lower costs. Manually managing identity-related tasks is not only costly in terms of administrative inefficiencies and productivity losses but can also lead to rubberstamping and increased cyber risk.

Enabling user access without compromising security, SailPoint Identity Security ensures that each identity has the right access needed to do their job- no more, no less. As a critical sector with complexity beyond human capacity, leveraging automation through AI-driven identity security is essential. SailPoint's AI-driven identity security ensures least privilege access, identifies anomalous access, prevents workforce access delays, and simplifies audit readiness. As a result, financial institutions can feel confident to accelerate their digital transformation and accommodate an expanding organization. SailPoint's identity security solutions are also flexible to meet you where you are with intelligent SaaS-based, on-premises, or hybrid solutions.

Improve your productivity, reduce operational costs, and secure against insider threats, external threats, and third-party risk. From the most sophisticated identity technologies with the scale to support the most complex, global enterprises, SailPoint can help streamline your identity journey and drive your financial institution forward. Learn more at https://www.sailpoint.com/solutions/industries/financial-services/.

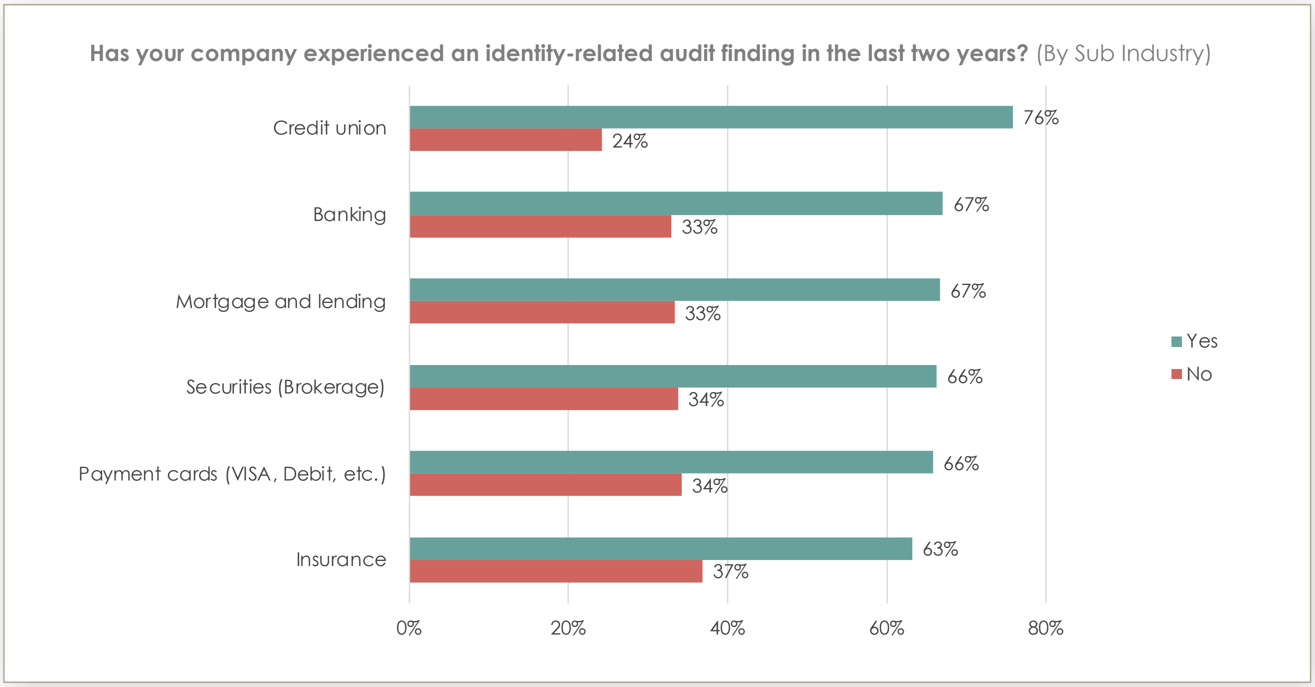
Most Financial Services Companies are Challenged to be Compliant

Similar to understanding the top identity security challenges, the research sought to also identify the top compliance issues. Unfortunately, 93% of financial services companies indicated challenges to achieving compliance. While changing regulations (48%) leads all challenges, there is not much companies can do to limit regulatory change. It still means, though, that companies need to quickly adapt to successfully achieve compliance. New compliance requirements mandate changes for people and processes, so their tools need to reduce burden and control risk. The next three answers: time-consuming (41%), requires significant resources (37%), and manual processes (37%), all indicate inadequate tools, which in fact appears later in the list with 27%. Even a lack of clear reports (28%) and not tracking outliers (18%) are tool issues, either lacking key functionality or signaling the tool is too hard to use.


At your company, what are the top challenges to achieving compliance?

Most Financial Services Companies Report Audit Findings

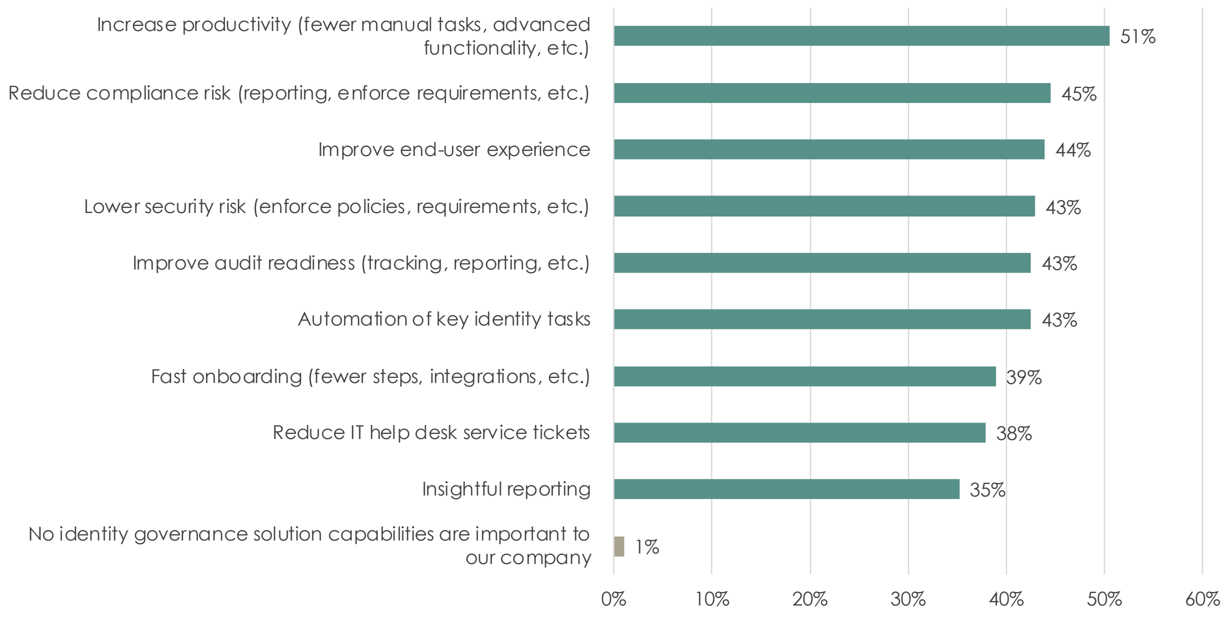
Audits usually provide validation that a company's processes and tools are meeting the compliance requirements; however, 64% of all financial services companies indicate they had an identity-related audit finding over the last two years. Audit issues can translate into a risk that can result in non-compliance or a breach. The fact that so many have audit issues should encourage companies to evaluate the top identity security and compliance challenges cited and determine whether they are contributing to the audit findings and if their tools have sufficient functionality to address them. In looking at the chart below is it interesting to discover that credit unions lead all financial institution service types by a significant margin.


Has your company experienced an identity-related audit finding in the last two years? (By Sub Industry)

Capabilities to Increase Productivity and Reduce Risk are Desired

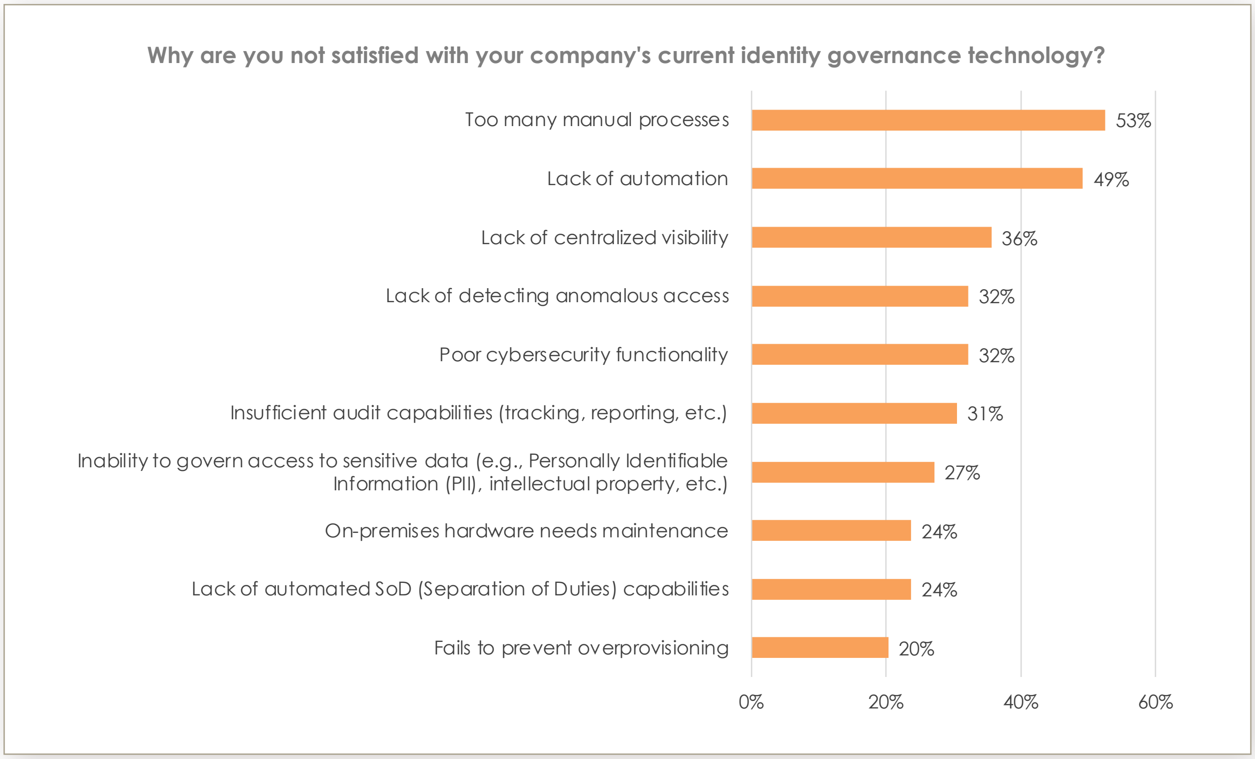
Several of the preceding sections and related findings directly and indirectly pointed at current identity security tools as being an issue. To further understand the issues, identity and security leaders were directly asked what solutions capabilities were critical to them. Leading these is productivity (51%), again indicating slow and numerous manual processes and the need for more automation and easier to use but more powerful tools. The next capability, reduce compliance risk (45%), typically can be distilled to proactive information about possible issues as well as enforcement of rules and policies. In the third spot, just one percentage point lower, is improved end-user experience (44%), which again is the need for easier to use tools. Many of the remaining answers reinforce that companies are looking for tools that drive efficiency and mitigate risk by utilizing tools with automation, increased functionality, and simplified proactive reporting.

What identity governance solution capabilities are important to your company?



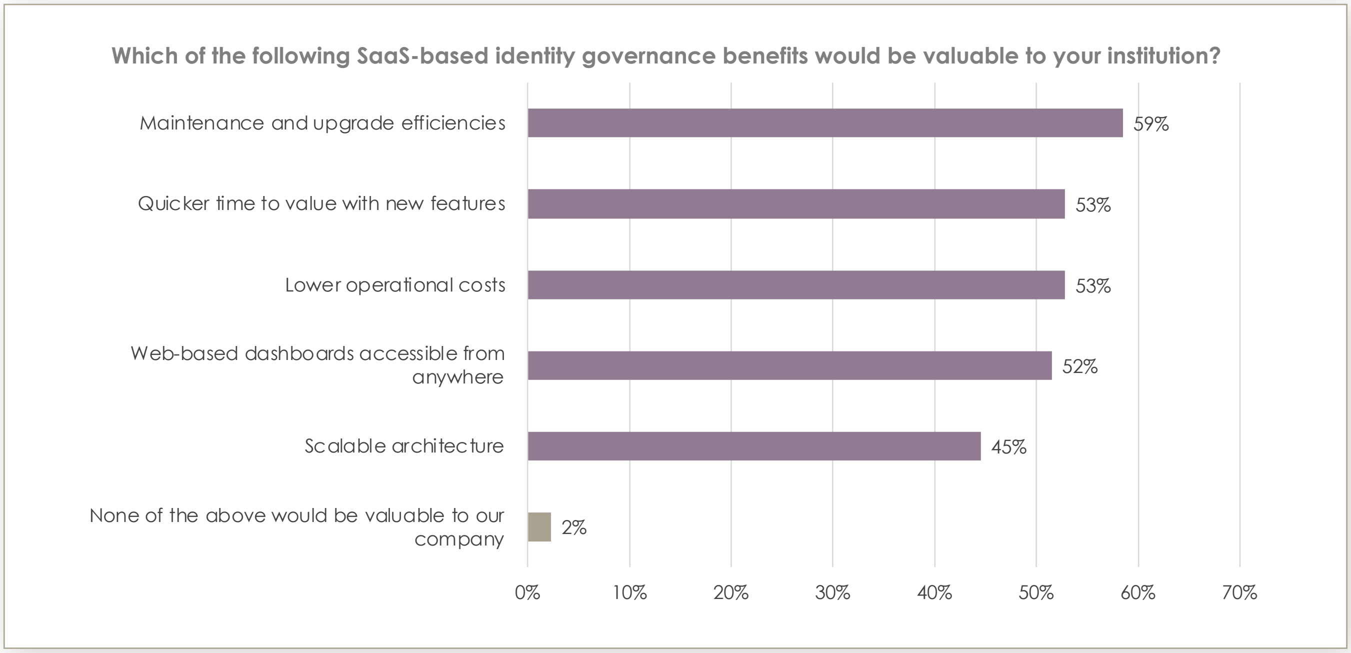
Current Identity Security Tools Lack Critical Capabilities

Given the long list of identity security solution feature needs, the research sought to gather direct feedback on their current tools and what they lacked. A pervasive trend persists with the top two: too many manual processes (53%) and lack of automation (49%), which are directly related. The other responses tend to reinforce the solution needs covered in the preceding section: lack of visibility (36%), and inability to detect anomalous activities (32%). Poor cybersecurity functionality (32%) provides some insight into how traditional identity management is evolving to identity security management. Many of the remaining dissatisfactions are about missing functionality, including poor audit capabilities (31%), inability to govern sensitive data (27%), lack of separation of duties capabilities, and failsafe for overprovisioning (20%).



SaaS-Based Identity Security Solutions Provide Tremendous Value

The research then endeavored to validate a theory that identity security solutions could provide more value in SaaS-based models. In short, 98% of IAM and security leaders indicated that they see benefits with SaaS-based identity security solutions, led by maintenance and upgrade efficiencies (59%). Given the complaints about current tools failing to provide needed functionality, it makes sense that 53% indicated value for quicker time to value with new features (53%). Perhaps as expected with SaaS solutions is lower costs (53%) and global access (52%). Scalable architecture (45%) completes the top five and likely addresses ever-increasing number of identities financial institutions face. Thus, SaaS-based identity security solutions appear to offer numerous benefits to close gaps with current tools.


Which of the following SaaS-based identity governance benefits would be valuable to your institution?

Conclusion

Financial services companies that are managing a growing number of identities are exposing gaps in how they are managing access and falling victim to breaches and incurring compliance audit findings. Numerous sections in this report indicate the identity security tools in use are inadequate, first lacking automation which results in slow, manual error-prone processes and increased risk. In addition, processes are too slow for large-scale identity increases from M&A as well as basic employee access needs which are impacting business. These manual processes are also driving the concerns about actively managing third-party identities properly which are growing in frequency and complexity and on which all financial institutions rely.

Manual processes and some current tools being used in financial institutions are hard to use and lack basic functionality such as clear reporting to help teams know if they are complying with compliance requirements. Additionally, the tools are not providing predictive insights of where risks are —that can lead to overprovisioning, a lack of separation of duties, third-party access, anomalous access — while the identity security team is buried with manual processes and simply lack the time to proactively look for them.

The tools teams are using today appear to be lagging in the evolution of identity security which requires identifying anomalous activities, identification, and management of access to sensitive data, centralized visibility, and direct security features.

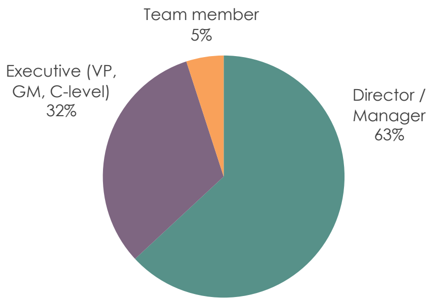
This research shows that identity security solutions in use by financial institutions are unnecessarily consuming resources, slowing the business, and failing to properly protect the business as half have had breach and/or compliance audit findings over the last two years. These events bring additional costs and, more importantly, damage customer trust in financial institutions that must secure both their money and their sensitive information. While the recommendation to upgrade to modern tools with automation to drive efficiency and mitigate risk seems obvious, a strong consideration should be of a SaaS-based solution that removes additional tasks from the team, such as upgrades and maintenance while providing the latest features with global access to manage identities with a proactive approach.

Survey Methodology

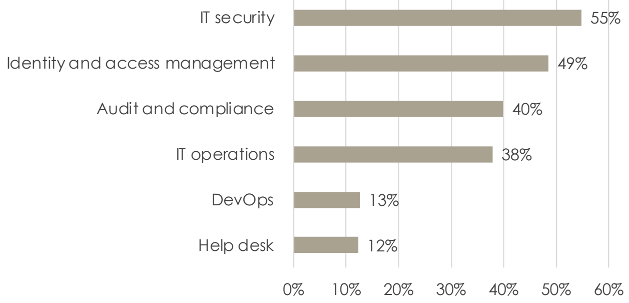
IAM, security, and compliance professionals at enterprise companies representing all seniority levels were invited to participate in a survey on their company's access strategy and management practices. The survey was administered electronically, and participants were offered a token compensation for their participation.

A total of **301 qualified participants** completed the survey. All participants had enterprise IAM and security responsibilities. Participants were from 5 continents representing a global perspective.

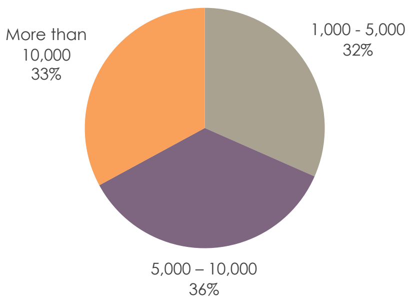
Seniority



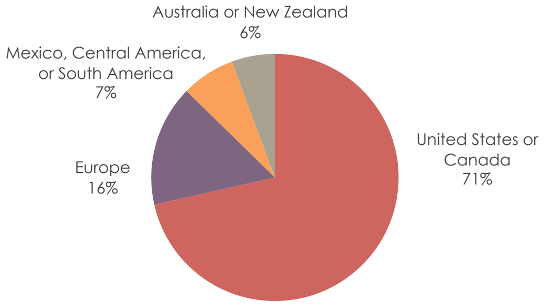
Responsibility



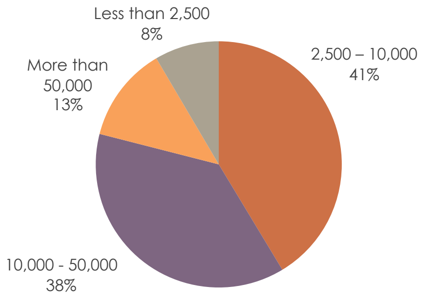
Size (employees)



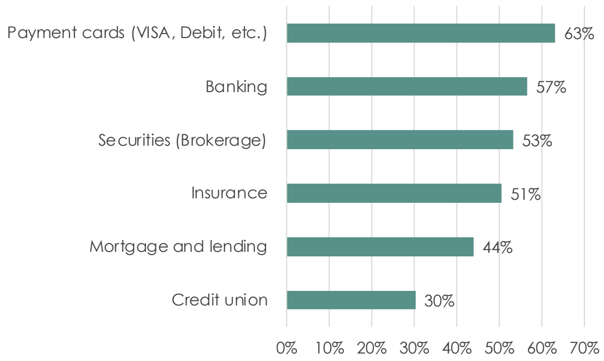
Location



Identities Managed



Financial Services Offered



About Dimensional Research

Dimensional Research provides practical marketing research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT and understand how IT organizations operate. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business.

For more information, visit dimensionalresearch.com.

About SailPoint

SailPoint equips the modern enterprise to seamlessly 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 highly complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.

For more information, visit www.sailpoint.com.