FORTRA

GUIDE (Core Security)

Doing Financial Services Identity Governance & Privileged Access Management Right

The Ultimate Guide for Managing It

Table of Contents

The Ultimate Guide Overview

Financial services organizations today face extraordinary challenges in a dynamic, complex landscape. During the last two decades, the financial services sector has seen increasing cybersecurity threats, data breaches, and cyberattacks. In fact, financial services companies are 300 times more likely than organizations in other sectors to experience cyberattacks, according to **CIO Dive**.

Organizations have also seen intensified regulatory compliance requirements, an acceleration of digital transformation, large-scale mergers and acquisitions, and the pressure to increase operational efficiencies and decrease overall costs, while meeting growing customer demands. Addressing these issues, while staying focused on delivering high-quality customer service, means these organizations must continually do more with less.

That's where Identity Governance and Administration (IGA) and Privileged Access Management (PAM) comes in—enabling organizations to intelligently and efficiently manage who has access to what systems and when, and deliver the most efficient path to mitigating identity risk.

Throughout this guide, we will explore key issues and trends within the financial sector that warrant the need for effective identity governance and privileged access management. We will examine the top drivers for IGA and PAM within financial services companies today. And we will provide actionable strategies for leveraging intelligent programs within financial institutions so they can mitigate risks, protect privileged accounts, and safeguard valuable data within their organizations.

Key Terms

Provisioning and Deprovisioning: The policy-driven setting up, removal, or changing of user access to resources and applications.

Access Certification: A process where managers, resource owners or individuals responsible for administering an application must review users who have access to that application. Commonly known as access reviews, this process includes an attestation that the user still requires, or no longer requires, access to the application. Unnecessary access is subsequently removed.

Roles: A collection of access rights on one or several applications that are grouped together because they are often assigned to the same types of users. When roles are defined, organizations can efficiently assign rights in automated fashion, while maintaining least privilege access policies.

Privileged Access Management (PAM): A critical security control that enables organizations to simplify how they define, monitor, and manage privileged access across their IT systems, applications, and infrastructure.

The Current State of Financial Services Information Security

Financial services information security continues to be a top priority across the entire financial sector—and for good reason. The **Verizon Data Breach Investigations Report** found that financial profit or gain was the primary motivation in 71 percent of all information security incidents, making financial services organizations a prime target for attack. With recent mega breaches occurring in the financial services industry, including the **Capital One breach** that revealed personal information of more than 100 million individuals, protecting sensitive personal information has never been more important.

According to **The Financial Matrix: Bitglass' Financial Breach Report**, of all the breaches that occurred across industries, only six percent of those breaches happened within financial services organizations, but more than 60 percent of all leaked records were exposed by financial institutions. One reason for this, according to the Verizon Data Breach Investigations Report, is that the use of stolen credentials on banking applications is common in financial services. In fact, 72 percent of data breaches across the financial sector arise from web applications, privilege misuse, and miscellaneous errors.

The rise of financial services technology (fintech), coupled with increased cyber threats and cyberattacks across the industry, means that these organizations must continue to pursue strategies and programs that protect sensitive financial information.

One of the most effective ways to secure sensitive information is through strategic Identity Governance and Administration programs and solutions that offer an intelligent path to mitigating identity and access-related risks. IGA helps ensure financial organizations have increased visibility into the identities and access privileges of their users, so they can intelligently and consistently manage who has access to valuable financial data and systems.

Just as important is protecting privileged accounts through Privileged Access Management (PAM) solutions. Because administrator accounts have elevated privileges that can access valuable financial data and execute applications or transactions—often with little or no tracking control—it can be very difficult to manage privileged accounts. PAM solutions centralize management of administrator profiles and ensure least privileged access is enforced to give users only the access they need.

Key Issues and Trends in the Financial Services Sector

To understand what financial services organizations are up against today, it is important to more deeply examine a number of challenges and trends in the industry. Below are five key issues that characterize the current financial services environment:

1. **Growing Cybersecurity Threats and Data Breaches:** Financial services organizations have been a constant target of cyberattacks and data breaches compared to other sectors. According to CIO Dive, these institutions are hit nearly 300 times more with cyberattacks than organizations in other sectors. Similarly, CISO Mag reports that '25.7 percent of all malware attacks last year were targeted on banks and financial organizations.' And according to the Verizon Data Breach Report, nearly one-third of data breaches were caused solely by stolen credentials. Stolen credentials are not only a risk from privileged accounts and active user accounts, but create an even greater risk from orphaned accounts, or those accounts within an organization no longer associated with a valid business owner that are not actively monitored.

When accounts within the financial services organization, especially privileged accounts, are not managed properly, and access is not governed appropriately, the institution can be more easily compromised and potentially lead to an increase in costly data breaches. The financial services sector has the secondhighest cost per breached record behind healthcare, averaging around $210 per record, according to CIO Dive, but a 'mega breach, like Capital One's, can cost up to $388 per record.' Protecting against these types of major data breaches should be top of mind for financial services organizations. Identity governance and privileged access management enables organizations to address the access challenges associated with these risks by intelligently managing user accounts and increasing visibility into the identities and access privilege of users, so they can better manage who has access to what systems, and when.

Pro Tip:

The Importance of Penetration Testing and Network Threat Detection

Financial services organizations are primary targets for attacks with the amount of sensitive data they protect. Leading institutions today regularly conduct penetration testing to increase visibility into the effectiveness of their defenses and reveal their most pressing risks, and then work to actively address those challenges. They also actively monitor their networks with network threat detection to ensure that alerts received are for verified attacks.

2. **Complex Regulatory Compliance:** Over the last two decades, and particularly since the 2008 financial crisis, the financial services sector has seen a complex web of regulatory compliance to ensure sensitive financial information is protected. Early legislation from the Sarbanes-Oxley Act (SOX) in 2002 introduced significant changes to regulating financial practices and corporate governance, while the Dodd-Frank Act of 2010 improved accountability and transparency across the financial system. As payment fraud began to increase, the Payment Card Industry Data Security Standard (PCIDSS) was established in late 2004, and has continued to intensify, with the current version of PCI-DSS 3.2.1 now mandating that organizations use multifactor authentication for all non-console administrative access.

   Mandates have increased in recent years and additional legislation has either gone into effect like the General Data Protection Regulation (GDPR) in the European Union, or the new consumer privacy law from the California Consumer Privacy Act of 2018 (CCPA) that went into effect in early 2020. Other recent developments like the New York State Department of Financial Services (NYDFS) also now require that all banks, credit unions, mortgage companies, insurance companies, and other financial institutions operating within New York to be registered or licensed by the DFS, and meet ongoing regulatory compliance.

   In addition to regulatory compliance, there are other regulatory frameworks, including Basel III from 2009, which oversees capital ratios that banks must maintain, the Current Expected Credit Losses (CECL) Methodology from 2016, which provided a new accounting standard across financial services organizations, and the more recent SWIFT standards, which went live in January 2020, requiring banks and financial houses to verify internally they are compliant with its new requirements.

Growing customer expectations will continue to place pressures on financial services organizations to increase the quality and efficiency of interactions, and to ensure sensitive financial information remains secure.

While not exhaustive, these standards and frameworks reflect that compliance today is not only more complex for financial services, but also more important than ever before. They require companies to collect information related to data access controls, and monitor activity related to financial information, authen-tication, and transmission security. Without proper identity governance and administration tools and privileged access management, reporting for regulatory compliance and frameworks becomes a tremendous burden for financial services organizations. This reinforces the need for financial institutions to leverage more effective and efficient security controls and systems to meet these increasing regulatory demands.

3. **The Rise of Digital Transformation:** Digital transformation has drastically changed the financial services sector within the last decade. Based on a definition from Salesforce, digital transformation is the 'process of using digital technologies to create new—or modify existing—business processes, culture, and customer experiences to meet changing business and market requirements. This reimagining of business in the digital age is digital transformation.' Compared to just 10 years ago, IT requirements today within financial services are vastly different based on consumer demand and advancing technologies.

For example, customers expect that they can easily check their banking transactions, anytime, anywhere. There are more systems connected than ever before to banking and investment houses. And there is more computing capacity required to manage these digital connections, which requires more governance and management of these systems, platforms, and accounts. Financial institutions operating in a digital world must continue to leverage technology-based solutions to address challenges in the industry, which is 'reflective of the industry-wide acceptance of digital transformation' replacing manual processes and systems, according to Hitachi Solutions.

BDO similarly reports that 'nearly 97 percent of financial services firms are making some sort of inroads on digital transformation,' with more than onefifth indicating it is the top digital priority in their organization. The benefits of digital transformation, according to BDO, include more effectively competing for customer loyalty, leveraging data driven insights, engaging new customers, and streamlining operations. In fact, the rise of fintech companies in just the last decade has rapidly changed the financial services landscape. In North America alone, the number of financial technology startups grew to more than 8,700 in February 2020, up from just over 5,600 in 2018.

Advancing technologies, including cloudbased platforms, infrastructure, Software as a Service (SaaS), and multi-application environments enable rapid scaling and growth within the financial sector. But with this digital transformation also comes considerable challenges for managing and governing access to those technologies.

The chaos that results from supporting countless devices, applications, and systems with access to key financial data is extremely challenging. And security teams find themselves struggling to keep up with the increasing demands of the business, with industry mandates, and with regulatory compliance. Financial services organizations must have the right access provisioning, management, and certification processes in place to ensure they are both complying with regulatory requirements and also mitigating—rather than magnifying—risk within their environments as the adoption of digital technology expands.

4. **Improving Customer Experiences and Retention:** Financial services customers expect secure, streamlined, personalized, experiences during their interactions with financial institutions. Growing customer expectations will continue to place pressures on organizations to increase the quality and efficiency of interactions, and to ensure sensitive financial information remains secure.

BDO emphasizes that customers 'will expect nothing less than real-time engagement when they need it. They will value simplicity, efficiency, and transparency. And they will not tolerate even the slightest possibility of a data breach.'

Ensuring breaches do not occur is essential to retaining customers. When breaches occur, companies not only incur the expense of the breach, they also typically lose customers in the process. According to a recent study featured in BankingDive, '66 percent of people surveyed said they would stop doing business with a company that had a slow or ineffective response to a data breach and would switch to a competitor. And 45 percent said they would tell their family and friends to stop doing business with the company.' Because mishandled employee access is responsible for a large number of breaches, organizations must prioritize protecting this access and make identity governance an essential part of overall data protection.

With so much expectation and scrutiny placed on organizations today, ensuring a frictionless process for delivering financial services is essential—and that requires the right identity governance programs and privileged access management to help protect access to the countless applications and systems that financial services use while interacting with customers.

Overarching challenges in the financial services industry create significant roadblocks for organizations today, and contribute to the need for establishing strong identity governance programs that help keep sensitive personal and financial information safe.

5. **Ongoing Merger and Acquisition Activity:** Within the financial services industry, mergers and acquisitions are a continuous part of the changing landscape. Last year, the value of M&A activity increased by 14 percent to more than $343.3 billion globally, with the year ending as the 'third most active year of deal flow by volume on record,' according to a **recent brief**. With more than 491 acquisitions in total last year, three of the largest deals involved U.S. firms exclusively. This included the acquisition of TD Ameritrade by Charles Schwab, worth more than $30 billion.

   While M&A activity levels may not reach the same amount this year as they did last year, **Deloitte** reports that 'escalating uncertainty won't bring banking and capital markets M&A to a standstill.' Instead consolidation will continue among small- and medium-sized institutions, and companies with strong balance sheets have more money to spend on investments and acquisitions,' further adding to the complexity of the financial services landscape.

   With financial services organizations constantly changing and the number of users and requirements to access multiple systems and resources continuously evolving, it is virtually impossible to manage this fluctuation without the right identity governance tools and privileged access management solutions in place. Identity governance adapts to ensure these types changes are more efficient and less risky within the climate of M&A. Larger institutional changes, like mergers and acquisitions or corporate reorganizations, can be streamlined through automated provisioning and approvals. This decreases the timeline to execute bulk additions, where a lot of change is happening at once and reduces risk associated with overseeing a high volume of user and privileged accounts.

These overarching challenges in the industry create significant roadblocks for financial services organizations today. And together, they contribute to the need for establishing strong identity governance programs that help keep sensitive personal and financial information safe. With these primary challenges in mind, let's now take a look at the top five drivers of identity governance and privileged access management for the financial services sector to more clearly understand how intelligent identity governance can address these challenges.

Top Five Drivers of Identity Governance and Privileged Access Management

Financial services organizations seeking to address the major challenges in their industry turn toward Identity Governance and Administration programs and Privileged Access Management solutions to more intelligently and effectively address their most pressing access-related challenges. Figure 1 represents the top five organizational drivers for financial institutions today and their needs for strong identity governance and privileged access management, including regulatory compliance, risk management, external pressures from organizational change, managing costs and driving high quality customer experiences, and improving IT service delivery.

Figure 1: The top five drivers for Identity Governance and Administration and Privileged Access Management in Financial Services Organizations today.

Financial services organizations seeking to address the major challenges in their industry turn toward identity governance and administration and privileged access management to more intelligently and effectively address their most pressing access-related challenges.

Financial services organizations leverage Identity Governance and Administration and Privileged Access Management solutions to automate manual processes and reduce the time required for auditing and reporting, enabling them to more easily demonstrate their ongoing compliance with regulations and industry mandates. They leverage IGA and PAM to manage risk more effectively and protect sensitive financial data from unauthorized access, eliminate excess privileges, protect privileged accounts, terminate orphaned accounts, and uncover segregation of duty violations within the organization.

In order to respond to continuous organizational change within the financial services sector, organizations look to IGA and PAM solutions to manage access-related activity for mergers and acquisitions, financial institution reorganizations, staffing changes, and employee changes or transfers.

Identity governance programs and PAM solutions also enable financial services organizations to mitigate identity risk, effectively manage privileged accounts, give the right levels of access to each person, reduce reliance on helpdesk support, and decrease audit-related costs for financial services teams. Finally, leaders seeking to improve IT service delivery can rely on IGA and PAM to onboard new hires faster, reduce administrative burden for managers, control privileged accounts, and streamline overall identity governance processes—enabling the organization to do more with less.

Critical Identity Governance and Privileged Access Challenges in Financial Services

Responding to the most pressing issues in the financial services industry, organizations in this sector have specific challenges they must solve to make their companies more secure in the face of ongoing change. Manual provisioning processes, insufficient visibility into existing account access, lack of control of privileged accounts, and the lack of automation significantly contribute to these challenges, magnifying the time and resources required to oversee and manage user access.

Because some organizations still lack a centralized process to manage and audit user accounts, they often have very little visibility into the actual access levels users possess. According to a **recent study**, only 53 percent of organizations today are confident in the effectiveness of their identity and access management programs. This translates directly to the challenges organizations in financial services face. With only half of all organizations today confident in their IGA programs, financial institutions face an upward climb to ensure their identity and access management is effective across their environments. Here are some of the top access-related challenges that financial institutions encounter today that can be addressed with improved IGA and PAM programs:

1. **Effectively creating and maintaining account access and privileged access across a disparate digital workforce:** With varying levels of access required for multiple user types across multiple systems, platforms, and devices, including privileged accounts within the organization, financial services security professionals must ensure they intelligently create, monitor, manage, and remove access in a timely manner. This also means securely and efficiently enabling appropriate levels of access across an expansive arrangement of locations, branches, and networks to enable users to effectively perform their jobs.

2. **Creating and managing the ongoing complexity and granularity of user roles and privileged accounts across titles, departments, and applications:** In addition to managing a diverse digital workforce, financial service organizations must ensure their IGA and PAM programs address the specialization and granularity of user roles across departments, titles, and user types. Financial institutions should operate with the policy of least privilege, while still providing users enough access to effectively perform their critical roles within the financial services organization.

Because some financial services organizations still lack a centralized process to manage and audit user accounts, they often have very little visibility into the actual access levels users possess.

3. **Addressing the time and resource requirements for provisioning:** The complexity of the financial services sector has contributed significantly to the time and resources required for user provisioning within organizations today. These growing demands continue to put strain on IT teams to keep up with provisioning and deprovisioning accounts, and ensuring appropriate levels of access are given to the right users.

4. **Ensuring customers receive frictionless experiences and securing sensitive financial information:** With increasing industry and government mandates around sensitive financial data, institutions must ensure they are continuously protecting data to meet ongoing regulatory compliance. This includes monitoring and prioritizing access risks, giving appropriate access levels to financial services staff and customers, and uncovering hidden access levels within the organization. Financial services organizations must also practice the policy of least privilege access so only those users that need access to data have it when they need it.

5. **Managing brand reputation, access risks, and trust:** Financial services organizations today know the value of keeping valuable financial information secure. And they also know the high cost that a data breach can have on their organization—both in terms of monetary costs and loss of brand reputation. Ensuring customers can trust their organization to keep financial information secure and providing streamlined interactions is essential to financial institutions today. By leveraging intelligent identity governance and privileged access management programs and solutions, organizations can elevate the value of their brand, and build ongoing loyalty and trust with customers.

The reality is that with so many systems and so many access privileges to manage, it is extremely difficult for financial services organizations to understand what access users need, and then control that access without the right identity governance programs. Research from Cybersecurity Insiders describes the complexity of access challenges today and the risk this presents to an organization. According to the **Identity and Access Management Report**, more than 70 percent of users have more access privileges than required for their job.

When employees and users have more access than they need, there is an increased risk of insider threats—whether accidental or intentional—and greater opportunity to target users with elevated access levels, magnifying risk across the organization. This risk becomes even greater if excess privileges are unused because nefarious access can go undetected. Combined together, these factors make it very difficult to limit risk within the business, especially in financial services organizations where institutional change and digital transformation is a constant.

Strategies for Leveraging Intelligent and Effective IGA and PAM Programs

The challenges that organizations face in relation to protecting sensitive data may seem overwhelming. But with the right strategies to guide their organization, financial institutions can leverage a best practice approach for identity governance and privileged access management. The following eight strategies provide a framework for financial services organizations to improve the quality and efficiency of their IGA and PAM programs, ensuring financial data security, protecting sensitive digital assets, and supporting ongoing compliance, so they can focus on what matters most—their customers.

Strategy 1: Simplify the Problem By Cleaning Up Your Environment and Harnessing Access Risk Intelligence

Companies that want to mitigate identity-related access risks should begin by leveraging intelligence to understand what risks are most pressing in their organization. In fact, the success of IGA and PAM programs can be greatly improved through analytics that increase visibility and insight into an environment. Gartner has indicated that those identity governance and administration implementations that begin with cleanup analytics demonstrate twice the ROI as those programs that don't. That's an incredible return for those financial services organizations willing to put in the hard work of 'getting their house in order' by using analytics to inform their identity governance processes.

Leveraging intelligent identity analytics helps identify risk and policy violations, so financial services organizations can put a plan in place to effectively begin critical cleanup. This is applicable not only to the risk that is easy to identify, but access risk that is hidden from direct view, or inherited in a complex environment. This cleanup sets the stage to address immediate threats, improve ongoing provisioning, and enhance governance and privileged access management across the enterprise.

The ability to immediately diagnose and reveal hidden access risks is paramount to simplifying access-related challenges. Once you have actionable information and insights, you can put a plan in place to effectively address your biggest identity risks. Financial services organizations seeking to leverage intelligence and simplify their access-related challenges should consider solutions that enable them to:

- ✓ *Diagnose access risks instantly, and gain actionable information and insights*
- ✓ *Get immediate visibility into hidden access risks within their network*
- ✓ *Easily identify orphan or abandoned accounts, unnecessary entitlements, or privileged accounts*
- ✓ *Establish a baseline for remediation specific to each company's most critical access risks*

Check out Core Access Insight later in this guide to find out how you can apply intelligence and analytics to quickly identify and evaluate access risks across your business critical-systems.

Strategy 2: Visualize Relationships Between Users and Access within the Complex Financial Services Organization

For organizations to understand the right levels of access to assign, what to change those levels of access to when necessary, and what to review them against, they should adopt a role-based approach that leverages role-based policies. As defined earlier in this guide, think of a role as a collection of access privileges typically around a job title or job function. Using roles, financial institutions can establish solid, predefined, and preapproved access policies and know specifically which access privileges each person needs.

This strategy simplifies identity governance and administration, and aids financial services organizations particularly as they grow and change. Embracing a role-based approach also decreases the timeline in executing bulk additions where a lot of change is happening at once, like during mergers and acquisitions and during corporate reorganizations.

Using an industry-leading role designing tool with cluster analysis and a 'visual-first' approach to group like-access privileges together, financial services organizations can better understand the access that individuals have in common and what outliers might be present. Financial services organizations that want more intelligent and visible identity governance across all of their environments should consider a visual-first approach that enables them to:

- ✓ *Easily view role definitions across multiple user types*
- ✓ *Gain insight into user access across the organization*
- ✓ *Determine whether overprovisioning or underprovisioning is occurring*
- ✓ *Identify whether similar users are receiving the right roles*

Check out Core Role Designer later in this guide to learn how you can accurately visualize relationships between users and access levels within your business.

Strategy 3: Automate Account Provisioning and User Lifecycle Management for Financial Technology Systems, Platforms, and Applications

Figure 2: The basic stages of the user lifecycle.

Establishing an effective IGA program requires automating provisioning around a user's lifecycle within the organization. This can start with the user's first relationship with the organization as a job applicant or employee, and conclude with the user separating from the organization. In between these events are multiple changes, and access requirements that must be closely managed. Within the user lifecycle, onboarding is typically the first step, where a new financial services employee receives initial accounts and access to the appropriate systems and applications.

Once onboarded, a user may need new or different access, particularly if transferred or promoted within the financial services organization. This occurs when a professional changes job roles or needs to perform different duties within a separate department or location—even temporarily. It can also include transfers to a new department or reporting to a new manager. The last stage occurs when a worker leaves the organization, either voluntarily or involuntary. For the latter, accounts should be quickly and automatically disabled, preventing any opportunity for the user to retain access to valuable financial data or credentials upon their departure.

Automating provisioning around the user lifecycle enables financial services staff to be productive on day one rather than waiting around for access. It also decreases the reliance on IT resources, while improving security by reducing the risk that access will be 'borrowed' during this period and decreasing the risk associated with manual provisioning and deprovisioning mistakes. At the very least, when provisioning automation is not practical or feasible, automated workflow and access policies for requesting, approving, tracking, and auditing should be deployed. Financial services organizations that automate provisioning around the user lifecycle should ensure this part of their identity program enables them to:

- ✓ *Create base access for new users from an authoritative source*
- ✓ *Remove user access based on direction from authoritative source*
- ✓ *Empower manager requests for user access*

Check out Core Provisioning later in this guide to learn how you can easily automate access requests and account creation in your financial services organization.

Strategy 4: Streamline Access Requests and Approvals to Increase Security and Efficiency Across the Financial Services Organization

For organizations to be successful in establishing effective identity governance programs, they need to leverage a onestop shop for user access. This strategy prescribes that financial institutions deploy one centralized portal to complete access requests and approvals. Providing a central hub for users to request additional access ensures financial services employees go through the proper channels for access to the expansive network of applications and platforms, and makes certain that proper approval and fulfillment policies are followed.

Pro Tip:
Leverage a centralized portal for user access requests and approvals.

Leveraging a centralized system makes it easy for users to request access, but it also provides a consistent method for creating accounts and entitlements consistent with internal policies and protocol. Financial organizations that streamline access requests should ensure this portion of their identity program includes:

- ✓ *A central platform for access requests and approvals*
- ✓ *The ability to streamline employee onboarding*
- ✓ *Automation to remove employees who leave the organization*
- ✓ *Functionality for integrated role management*

Check out Core Access later in this guide to learn how you can streamline access requests and approvals in your organization.

Strategy 5: Simplify the Access Review Process and Respond to Ongoing Regulatory Compliance

Organizations that view regulatory compliance through the lens of an IGA program recognize they should monitor access continuously and provide access to only those individuals that need it, enabling the organization to stay more compliant. IGA solutions not only ensure access to information like financial data is strictly controlled, but also enable financial institutions to prove they are taking actions to meet compliance requirements. Conducting frequent access reviews or certifications is a key area for enhancing identity governance.

Within the climate of regulatory compliance, especially increasing auditor demands, it is imperative for financial services organizations to review user access periodically. Access reviews must be simple and easy to complete. If they are not, managers and reviewers may have the tendency to approve access in bulk to save time, also known as rubber stamping their approvals.

While some organizations still use a manual process, passing around spreadsheets among reviewers, a more intelligent, visual approach is a must-have to start grouping like-access privileges together. This enables managers across financial institutions to understand which users have access to specific systems, and which users are outliers in their privileges. Leveraging an easier review process leads to greater accuracy, improved reporting, and greater adoption within the organization.

Another key element for financial services organizations to consider as part of their review process and broader IGA program is micro-certifications. Since the time between new provisioning and the next audit or review process can be fairly lengthy, it is important to have a set of controls that can quickly identify anomalous access, especially when that access violates an important policy, such as segregation of duties or privileged access. This can be done through the use of micro-certifications.

Pro Tip:
Take advantage of automated micro-certifications to ensure any new or revised access or entitlements can be reviewed immediately.

Micro-certifications allow managers within the organization to be alerted when an employee may have new or updated access and entitlements other than what is expected, or if staff gain access through an outside process, commonly referred to as out of band. This alert allows the approver to perform an immediate access review associated with the event, significantly reducing any chance of insider threats within the system, enabling the financial institution to meet ongoing regulatory compliance, and allowing for any exceptions that might be necessary. Financial services organizations seeking to streamline the access review process should ensure an automated certification process empowers them to:

- ✓ *Easily identify and manage access rights for applications*
- ✓ *Conduct access certifications to applications and file shares*
- ✓ *Remediate inappropriate or high-risk access*
- ✓ *Respond to compliance audit demands*

Check out Core Compliance later in this guide to learn how your financial services organization can automate access certifications.

Strategy 6: Streamline and Centralize Privileged Access Management Across IT Systems, Applications, and Infrastructure

Financial services organizations struggling to achieve effective protection of privileged and root accounts often wonder what the best approach to Privileged Access Management is for their business. Privileged accounts are considered elevated accounts within the IT environment that hold the 'keys to the kingdom.' These types of accounts frequently have privileges to access valuable data and execute any application or transaction, typically with little or no tracking or control. A privileged account can take the form of an Administrator in Windows environments or Root in UNIX or Linux environments.

Privileged Access Management is a critical security control that enables financial services companies to simplify how they define, monitor, and manage privileged access across their environment. With full control over privileged accounts, IT and security teams within the financial services organization can help prevent internal and external attacks on critical systems before they start.

Organizations in the financial sector that want to centralize management of their privileged accounts, secure systems without slowing down productivity, and easily enforce least privileged access look to PAM solutions specific to their multi-platform environment. A strategic PAM solution provides all the components needed for effectively protecting privileged and root accounts both proactively and adaptively.

Leveraging PAM solutions simplifies the ability of financial services organizations to enforce security policies, control elevated access to critical systems and information, and provide full control over accounts, access, and privilege.

What Are PASM and PEDM?

As Privileged Access Management has evolved, Gartner has established two further classifications to highlight different mechanisms of PAM solutions. These include Privileged Account and Session Management (PASM) and Privilege Elevation and Delegation Management (PEDM). PASM and PEDM are two categories of security tools that have distinct approaches in how they manage access.

Both PASM and PEDM tools use the principle of least privilege, which mandates that users only have the access necessary to their job functions. While both solutions have the same goals, they have different mechanisms in how the target account is protected and accessed.

PASM: PASM solutions are often referred to as password vaulting. Privileged account credentials are securely created and distributed exclusively by the solution. When users need access to a specific server, they request access from the vault, and are given a temporary account with full administrative privileges. This account is only valid for a single session. Additionally, the session activity is monitored and recorded.

PEDM: PEDM solutions distribute access privilege based on job roles. Instead of using temporary privileged accounts, PEDM tools assign permanent privilege to standard accounts. PEDM tools define who can have access to each part of a system as well as what they can do with that access.

Financial services organizations seeking to centralize management of their privileged accounts should ensure a commercial PAM solution enables them to:

- ✓ *Improve security with granular access controls*
- ✓ *Enforce security controls across a multi-platform environment*
- ✓ *Give users only the access they need and ensure that least privileged access is enforced*
- ✓ *Enable scalability to centrally manage all aspects of account provisioning, access control and privilege escalation*

Check out Identity & Access Manager (BoKS) later in this guide to learn how your financial services organization can centralize management and effectively control privileged accounts in your business.

Strategy 7: Enforce Strong Password Management Across the Financial Services Organization

Pro Tip:
Empower users to leverage self-service mechanisms for password resets, like SMS, mobile app, or telephone.

With so many systems, applications, platforms, devices, and users, it can be difficult for organizations to ensure employees are regularly changing their passwords, so it is important to have frequent mandatory password resets. It is also important to maintain password policies that enforce complexity and non-reuse rules. However, the problem with password resets is that users may forget their newly updated passwords, requiring additional IT resources to support a simple reset—taking valuable time away from focusing on more strategic business initiatives. One way to combat this challenge is to leverage a strong self-service password solution that enables financial services professionals to securely reset their own passwords.

Leading password reset solutions allow users to also unlock their accounts through selfservice mechanisms. A variety of password reset options, such as a mobile reset application or telephone-based keypad resets, Windows Credential Provider and voice biometrics help increase user adoption rates, while maintaining a secure reset channel. Financial institutions seeking to improve the strength of their overall identity governance program should enforce strong password management across the organization and look for a solution that:

- ✓ *Delivers faster, more convenient user self-service*
- ✓ *Synchronizes passwords on multiple systems*
- ✓ *Reinforces strong password policies*
- ✓ *Reduces password-related help desk calls*

Check out Core Password later in this guide to learn how your financial services organization can empower users with a self-service password solution.

Strategy 8: Reduce Certification Fatigue and Increase User Adoption within the Financial Services Organization

Reviewing entitlements without adequate user context is overwhelming within the expansive network of a financial institution. Yet this is a common practice and can lead to inaccuracies and excessive distribution of access across the workforce. Underprovisioning financial services professionals can also lead to increased risk and a lack of productivity if credential sharing occurs or specific users do not have the right access to do their jobs. For financial services organizations to build a more effective identity governance program, they must empower managers and approvers to simplify the review process.

Pro Tip:

Add context to access reviews and certifications by leveraging a visual-first approach that compares access between users.

And one of the best strategies to do this is through streamlined visualization of common user entitlements. This enables reviewers to quickly and easily compare access to others, adding essential context during the review process. Increasing operational efficiency also results in higher user adoption rates across the organization—and that goes hand-in-hand with increasing overall security posture. Financial services organizations that make it part of their overall strategy to reduce certification fatigue through a more contextual and visual solution solve the essential challenges related to:

- ✓ *Requiring approvers to conduct too many certifications*
- ✓ *Manually certifying user access across multiple user types*
- ✓ *Providing insufficient contextual information about user access*

Check out Core Certify later in this guide to learn how your financial institution can reduce certification fatigue and create a visual approach to access certifications.

Leading-Edge Identity Governance and Privileged Access Management Solutions for Financial Services Organizations

Financial services organizations have unique needs and requirements when it comes to identity governance and privileged access management. And Core Security understands this. Financial institutions require intelligent solutions to address their expansive digital networks, systems, and applications. They need to automate provisioning across a disparate workforce. And they need to secure critical financial data and information, while demonstrating ongoing regulatory compliance.

Core Security is a leading provider of Identity Governance and Administration and Privileged Access Management solutions to the financial services industry. Our solutions streamline access management, reduce the overall threat surface, decrease IT costs, and support compliance for financial institutions of all sizes. The Core Security solution portfolio includes two suites and a leading-edge privileged access management solution that have been recognized by industry analysts, including Gartner.

Access Assurance Suite

- Core Access
- Core Provisioning
- Core Compliance
- Core Password & Secure Reset
- Core Access Insight

Visual Identity Suite

- Core Certify
- Core Role Designer

Identity & Access Manager (BoKS)

Figure 3: Award-winning solution components of the Core Security IGA and PAM Portfolio

How Core Security Offers Leading-Edge Identity Governance and Administration and Privileged Access Management Solutions

Core Security provides the most efficient path to mitigating identity risk within financial service organizations today. Our intelligent IGA and PAM solutions enable companies in the financial services sector to improve security, boost efficiencies, and ensure ongoing compliance.

Here's a glimpse at how our portfolio of award-winning IGA and PAM solutions make an impact for financial services organizations today:

- Improve quality of customer service by ensuring financial services professionals have the right access to the right systems, applications, and resources
- Enable effective rollout and expansion of digital fintech solutions and meaningful use programs by providing seamless user access to all relevant applications and data
- Avoid potential audit findings from regulatory compliance and industry mandates by adopting tools to detect and correct inappropriate access and behavior
- Leverage our depth of expertise in the financial services sector to ensure program success without diverting resources from customer services
- Adopt a phased implementation approach that enables financial services organizations to realize identity governance solution benefits quickly

Core Security Solution Portfolio

Access Assurance Suite

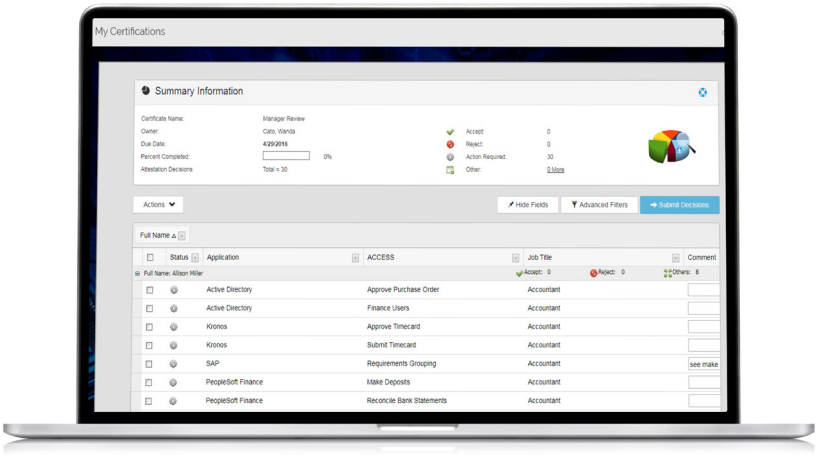
An integrated identity governance solution that delivers informed provisioning, continuous compliance, and actionable analytics. Comprised of four industry-leading modules, the Access Assurance Suite enables financial services organizations to streamline the provisioning process, review access requests, easily manage compliance, and enforce robust password management in one complete solution.

- **Core Access:** A convenient web portal where end users can request access and managers can review, approve, or deny access. Using a shopping cart approach, Core Access delivers an efficient and user-friendly experience—replacing paper forms, emails, and tickets used to manage access. Plus the ability to leverage roles enables access to be assigned quickly and accurately.

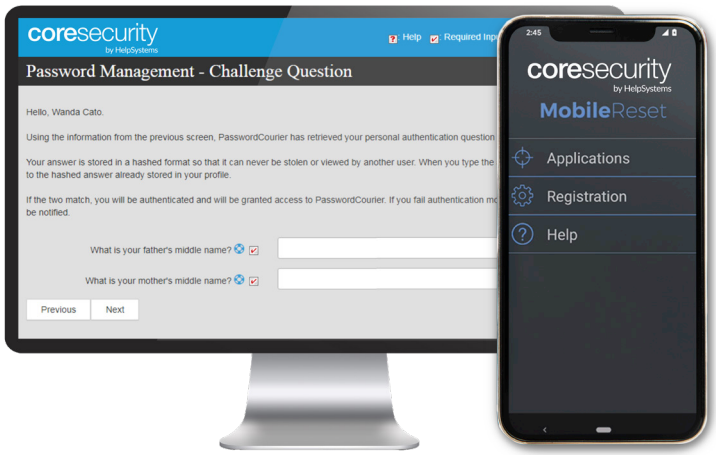
- **Core Provisioning:** As the backend fulfillment engine for Core Access, Core Provisioning uses software connectors to programmatically create and manage user accounts based on policies and permissions set up in Core Access. Our solution offers automated provisioning actions on hundreds of applications used across industries, organizations, and departments.

The Access Assurance Suite is a good choice for organizations that require a balanced approach to provisioning and access governance, with built in support for analytics.

Gartner Critical Capabilities for Identity Governance and Administration



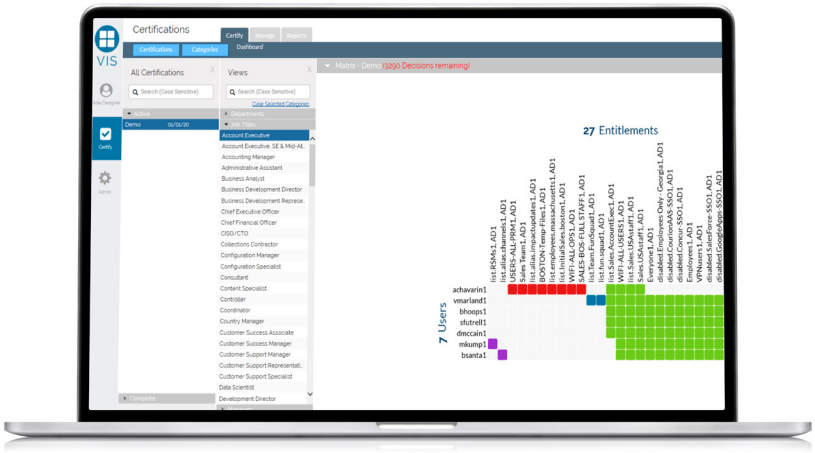
- **Core Compliance:** Identify and manage access rights for systems, platforms, and applications in a single interface, eliminating the need to review spreadsheet after spreadsheet. Immediately respond to compliance audit demands to ensure adherence to regulations like SOX, PCI-DSS, and GDPR.



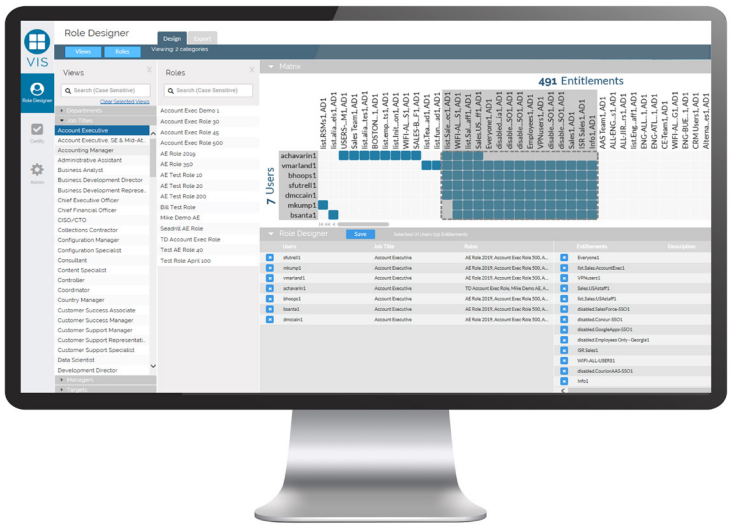
- **Core Password and Secure Reset:** Core Security provides a complete, integrated solution for automated password management. Core Password and Secure Reset work together to provide a convenient and secure password reset solution for your organization. Leverage simple, secure self-service password resets to automate password management and reduce access risks. Easily enforce robust password policies and empower users to streamline security in your organization.

Visual Identity Suite

See privileges and certifications in a whole new way—leveraging a visual-first approach. Our graphical user interface enables administrators, managers, and users to make informed decisions through the use of dynamic dashboards. Quickly see common user entitlements, identify outliers, and ensure the right people have the right access to the right systems. Visual Identity Suite is offered in a cloud delivery model and works with any Identity Governance and Administration solution.



- **Core Certify:** Delivers a visual-first approach by automatically clustering like-access together to simplify the access review and certification process. As part of this clouddelivered suite, managers can now accept or reject clusters of access—with just a few clicks—saving time, increasing accuracy, and reducing certification fatigue.



- **Core Role Designer:** A modern way of building roles. With Core Role Designer, it is easy to see patterns of access that should define roles by examining the clusters of access across individual users. Common access clusters establish a clearly defined role.

Core Access Insight

Access Insight offers a continuous, comprehensive view and analysis of the relationship between identities, access rights, policies, and resources that occur across your entire environment. Our easy-to-use solution applies analytics to the big identity and access data in your organization, empowering you to identify risks, and drive provisioning and governance controls to manage that risk within your business.

- *Evaluate and act upon risks associated with user access and activities*
- *Easily identify and remediate improper user access that could harm your organization*
- *Analyze massive amounts of identity and access data against policies*
- *Make informed decisions about the appropriate access designated to each role in your organization*
- *Understand complex access structures through intuitive visualizations*

Access Insight works with the industry-leading portfolio of solutions from Core Security, or in conjunction with other IGA solutions, to identify potential risks to the business, so you have a continuous and comprehensive view of your network and can quickly modify access as needed.

Identity & Access Manager (Boks)

Identity & Access Manager (BoKS) is an identity, account, and privileged access management platform that simplifies your organization's ability to enforce security policies, and control access to critical systems and information. BoKS transforms your multi-vendor Linux and UNIX server environment into one centrally managed security domain and simplifies your organization's ability to enforce security policies, and control access to critical systems and information. With full control over accounts, access, and privilege, IT and security teams can proactively prevent internal and external attacks on critical systems before they start.

Intelligent Identity Governance in Action

When a large national bank experienced rapid expansion of its banking services across multiple locations, its aggressive growth strategy put a strain on provisioning, compliance process, and infrastructure. Manually provisioning employee access to new systems or revoking access based on changing employment status limited productivity and created risks to the security and privacy of customer data.

The process of manual provisioning also became disconnected from business processes, making documentation for audit and compliance cycles difficult to manage. To address these challenges, the bank sought a solution that could meet its specific access provisioning and compliance goals, including automating provisioning processes, eliminating the quarterly profile review and attestation process, maximizing existing administration staff and technology including integration with existing workflows, and meeting regulatory requirements and federal mandates such as Sarbanes-Oxley and the Gramm-Leach-Bliley Act.

The bank selected Core Security Identity Governance and Administration solutions to automate role-based provisioning and access compliance verification to ease documentation requirements for audit and compliance cycles. A new workflow was also developed for HR to terminate users outside the standard scheduled workflow, allowing system access termination at any time for an employee whose status had changed. This immediately alleviated security exposure and privacy risk.

Soon after going live, the bank experienced increased efficiencies by automating policy enforcement and role management tasks along with streamlined operational and business processes associated with onboarding and offboarding staff. With the ability to automatically ensure compliance with business policies, the need for quarterly profile reviews has been virtually eliminated.

The bank also improved business processes outside of traditional provisioning by creating operational efficiencies associated with time-consuming security procedures. This was accomplished by creating new workflows to enable remote access for employees, while maintaining alignment with business requirements and complying with information security policies.

Start Your Journey to Intelligent Identity Governance and Privileged Access Management

There is too much at stake for financial services organizations today to ignore the importance of implementing an intelligent identity governance program and privileged access management solution that mitigates access-related risks across the business. Investing in IGA and PAM solutions from Core Security enables financial institutions to significantly decrease their risk of attack, supports streamlined regulatory certification and compliance, and increases operational efficiencies—keeping valuable data safe and keeping organizations focused on providing exceptional experiences to customers.

Ready for IGA and PAM solutions that protect your organization in the face of change?
Get a live demo of Core Security Identity Governance and Administration and Privileged Access Management solutions from one of our experts today.
www.coresecurity.com

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.