CUSTOMER SUCCESS STORY

SailPoint
MANAGING THE BUSINESS OF IDENTITY

Strengthening Control over User Access

FINANCIAL SERVICES

CHALLENGE

As one of the largest commercial banking companies in the United States, the company offers every financial service from retail banking to asset management and foreign exchange. The company faces rigorous requirements for regulatory compliance, security and risk management and needed better visibility and stronger controls over user access privileges.

SOLUTION

The bank implemented SailPoint IdentityIQ across its business-critical applications and 30,000 users to fully automate its access certification process. Integrating user access reviews in a single system eliminated orphan accounts and helped the customer to remove inappropriate access privileges that increase security risks.

As one of the largest commercial banking companies in the United States, the bank's growth came largely from acquisition of many companies. As the bank expanded, so did the challenges of managing its ever-growing and increasingly complex IT infrastructure — especially keeping track of which workers had access to critical data and applications.

The management team realized that its growth was outstripping its ability to ensure that strong internal access controls were in place and in compliance with federal regulations such as Sarbanes-Oxley (SOX), Gramm-Leach-Bliley and other federal laws governing financial institutions. The bank had a cumbersome, inefficient process for reviewing and certifying user access and did not provide adequate information to reviewers, making it hard to provide effective oversight. In the past, the bank had deployed a user provisioning solution, but this system did not provide the coverage to the critical back-office systems that are the focus of its compliance and risk management processes.

The bank wanted to strengthen its controls over user access privileges and to spend less time on manual data collection and reporting. After reviewing other solutions in the market, the company chose SailPoint IdentityIQ™ to replace its manual access certification efforts. IdentityIQ created a common identity governance environment that clearly showed all user access to sensitive applications at the detailed privilege level, enabling business managers to make informed decisions about allowing or revoking privileges.

Since implementing SailPoint IdentityIQ, this customer has been able to:

- Consolidate all of its identity data for critical, regulated applications into a single repository
- Replace manual processes with automated reporting and approval workflows
- Improve the quality of information in access certification reports
- Gain enterprise-wide visibility over and control of access privileges
- Reduce insider threat risk by removing 10 percent of access privileges as inappropriate

Quick wins forecast long-term success

Better visibility into access privileges

The bank implemented SailPoint IdentityIQ to proactively manage the risk of theft or damage from an insider misusing their access privileges. A key objective for the IdentityIQ implementation was to replace a semi-manual access certification process, based on spreadsheets and e-mail, with automated workflows that circulated easy-to-read reports from IT to business managers and back. Before IdentityIQ, the IT staff periodically compiled lists of users and their application accounts into Excel spreadsheets and e-mailed them to business managers. The business managers reviewed and approved the spreadsheets and sent them back.

The "Excel over Outlook" system gave visibility into account-level access, but the reports didn't show managers what users could do once they had access to an application. The lack of detailed entitlement information made it almost impossible for managers to identify inappropriate privileges or toxic combinations of access. A big priority for the bank was getting business managers more actively involved in the certification process so that the burden of managing enterprise risk was shared by business and IT managers. The bank believed that business managers needed to collaborate with IT because they were better able to judge whether a worker's access privileges are appropriate to his or her job. By implementing IdentityIQ, the bank was able to provide managers with reports showing low-level access privileges in a business-friendly format. Combining business managers' knowledge of organizational roles with IT managers' knowledge of applications in one system gave the bank precise, enterprise-wide control of access privileges.

Rapid deployment for complex enterprise applications

The first phase of the bank's IdentityIQ implementation focused on automating and streamlining the access certification process. Over a 15-week period, the company deployed SailPoint IdentityIQ for data aggregation and correlation, access certification and reporting across its business-critical mainframe and distributed applications. As part of the process, business and technical managers reviewed the naming and descriptions of all access profiles for accuracy to ensure that business managers had the right information to make informed decisions during certifications.

Featured SailPoint Capabilities

FEATURE	FUNCTION
Identity Data Aggregation	Aggregates technical identity data scattered across multiple enterprise systems and transforms it into a centralized, easily understood and business-relevant format that's accessible and actionable.
Identity Data Correlation	Correlates user identities across systems and applications using rule-based algorithms.
Consolidated Certification Reporting	Centralizes access data, including entitlements, roles and policy violations, across the organization and formats it into easy-to-read certification reports.
Automated Workflow	Automates certification process for routing certification requests, including approvals, delegations and remediation requests.
Business-oriented Certification Process	Enables organization to distribute certification decisions to business users by simplifying the presentation of complex IT access data.

Business-friendly reports enhance accuracy to improve overall compliance performance

Once a solid baseline of reliable identity IT data was established, the bank launched a fully-automated access certification process. SailPoint IdentityIQ automatically produces certification reports in an easy-to-read format with check boxes next to each item requiring review. The solution routes the reports to business managers, who certify and modify access data on a quarterly basis. At the end of the process, IdentityIQ produces a list of changes and remediations that are needed.

Lessons learned

Based on the successful deployment experience at the bank, SailPoint offers the following suggestions for best practices:

Include all stakeholders in the process

Implementing an access certification project requires a collective effort from IT, Business, and Compliance/Audit staff. Business managers need to be educated on the benefits of the project because they will be the primary users of the new tool. The implementation will also require the support of IT and compliance/audit teams, so engage them early in the process to gain their buy-in.

Scope the project carefully

Scoping an identity governance project carefully can help ensure its success. An access certification project can be as big or small as deemed appropriate. It can span the entire organization or include just a few key applications. Deploy your project in phases, allowing your team to get buy-in along the way by showing incremental results.

Start by building a solid foundation

The starting point for any identity governance project is centralizing and cleaning up your identity data. This process is designed to resolve any inconsistencies and inaccuracies between the various sources of identity data, creating an enterprise-wide view that will enable you to implement appropriate controls and better manage risk. Time invested during this phase will help ensure your success as you build out additional compliance tasks.

Recognize that provisioning may not be the right solution

Provisioning tools do not easily adapt to the requirements of access certification and identity governance. They can be complex and costly to deploy to large numbers of business applications, and they do not provide business-friendly interfaces needed to support compliance processes. As many customers like this one have learned, provisioning is not the best option for meeting governance and risk management requirements.

Making better decisions in less time

SailPoint has enabled the bank to translate technical identity data into easy-to-understand access privileges mapped to over 30,000 users. It has empowered business managers to approve and deny access privileges of their employees when necessary. That works because IdentityIQ maps low-level access privileges to roles and presents them in a business-friendly format.

The bank's access review is more reliable and its exposure to risk minimized because it now has a sound process for ensuring the company's workers have appropriate access privileges. The bank's previous method of doing certifications was not practical for a company of its size and complexity. Even if staffing a manual system wasn't an issue, the old system simply didn't provide the visibility, control and agility the bank needed to aggressively manage their internal risk.

SailPoint's level of automation gives the bank responsiveness and detail in a business-friendly context helping it to make better decisions in less time. IdentityIQ's automation and enterprise-wide view of access has eliminated rudimentary data gathering, and ultimately has made auditing for regulatory compliance faster and easier.

A look ahead

Looking ahead, the bank plans to expand coverage with SailPoint to include an additional 80 SOX-relevant applications. The company also plans to enhance its compliance performance by automating the enforcement of corporate access policies through cross-application Separation-of-Duty (SoD) rules. And to continue its efforts to align IT compliance with business processes, the customer plans to expand its business role modeling and ongoing role lifecycle management.

The SailPoint advantage

Taking a risk-based approach to governance and compliance, SailPoint helps organizations prioritize and focus internal controls and audits — ultimately reducing compliance costs and resource burdens.

Support compliance through improved role management

SailPoint uses a flexible, automated approach to help organizations create, enforce and verify role-based access across diverse enterprise applications. Comprehensive role management functionality makes it easy to determine who has access to what data; whether the access is appropriate; what users are doing with that access; and if they are in violation of established business policies or regulatory requirements.

Strengthen security with better visibility

SailPoint's unique risk-aware approach provides a 360-degree view of user access that establishes critical linkages between each user's identity, access privileges and job duties. Armed with this identity intelligence, enterprises can determine the relative risk a user's access poses to the business and transform technical identity data into meaningful insights business managers need to make effective decisions. Executives can confidently address the stringent reporting requirements of auditors and compliance staff.

Balance IT and business goals

Successful governance, risk and compliance (GRC) initiatives demand collaboration across both business and IT stakeholders. SailPoint offers the first and only identity governance solution offering a collaborative tool that enables business managers and IT staff to define a top-down business model for complying with internal policies governing users and their access privileges.

Corporate Headquarters
11305 Four Points Drive
Building 2, Suite 100
Austin, Texas 78726
512.346.2000
USA toll-free 888.472.4578
www.sailpoint.com

Global Offices

UK	+44 (0) 845 273 3826
Netherlands	+31 (0) 20 3120423
Germany	+49 (0) 69 50956 5434
Switzerland	+41 (0) 79 74 91 282
Australia	+61 2 82498392
Singapore	+65 6248 4820
Africa	+27 21 403 6475

About SailPoint

As the fastest-growing, independent identity and access management (IAM) provider, SailPoint helps hundreds of the world's largest organizations securely and effectively deliver and manage user access from any device to data and applications residing in the datacenter, on mobile devices, and in the cloud. The company's innovative product portfolio offers customers an integrated set of core services including identity governance, provisioning, and access management delivered on-premises or from the cloud (IAM-as-a-service). For more information, visit www.sailpoint.com.