CUSTOMER
SUCCESS STORY

SailPoint
MANAGING THE BUSINESS OF IDENTITY

Sallie Mae Reduces Compliance Pressures with Identity Governance

FINANCIAL SERVICES

OVERVIEW

The nation's leading provider of saving and paying-for-college programs, Sallie Mae services billions of dollars in education loans and college-savings plans and provides a variety of related services to government agencies and other clients. As a public company handling sensitive financial data, and as a federal government contractor, the company faces significant regulatory compliance pressures.

CHALLENGE

Sallie Mae needed a cost-effective alternative to expensive manual processes for demonstrating compliance with federal regulations such as SOX, PCI, and FISMA, and for conducting SAS 70 audits.

SOLUTION

Sallie Mae chose SailPoint IdentityIQ to improve compliance performance while saving time and money. The new automated processes eliminated time-consuming spreadsheets and cumbersome manual reviews, simplified IT administration during access certification, and improved oversight into identity data.

Sallie Mae is the nation's leading saving, planning, and paying for college company, helping millions of Americans achieve their dream of a higher education. Formerly known as SLM Corporation, the company and its subsidiaries offer a range of financial products, including college savings. The company services $202 billion in education loans and $27 billion in college-savings plans. It also provides related services and products to government agencies and other business clients. Because Sallie Mae is a public company dealing with sensitive financial data, it must comply with industry regulations and standards including SOX and PCI; it also conducts SAS 70 audits. As a federal contractor, Sallie Mae must additionally comply with FISMA, which governs federal information security management.

These compliance mandates can be a quagmire for Sallie Mae's IT resources and budgets. As part of an effort to address spiraling compliance costs, Sallie Mae began an aggressive identity governance project in December 2009. Within six months, the company had completely re-architected its IT compliance processes related to identity management and established an automated, repeatable process that is projected to save considerable expense while improving the company's overall IT risk and compliance posture.

With SailPoint, Sallie Mae has been able to streamline identity governance processes. SailPoint IdentityIQ™ has enabled the company to improve compliance by automating core compliance activities and managing role-based access control to increase the accuracy and efficiency of its access certification processes. At the same time, the company has reduced its business risk by establishing a high level of visibility into user access privileges to identify and monitor high-risk user populations.

Since deploying IdentityIQ, Sallie Mae has been able to:

- Automate cumbersome manual processes for access certification
- Simplify the IT administration required during certifications
- Improve the company's level of oversight into identity data
- Bring much-needed visibility into user access privileges
- Pave the way for self-service access request capabilities

Improving access certification

Sallie Mae's principal goal was to better address strenuous FISMA compliance requirements, and at the same time address all other regulatory requirements. The regulations make it necessary for the companies to demonstrate their ability to protect the integrity of IT systems by preventing and detecting unauthorized or inappropriate access to critical information. Effective identity management can help meet this goal by defining processes for granting, modifying, and removing access. To that end, Sallie Mae used IdentityIQ to automate the access certification process and simplify the reports that business managers were being asked to review and validate.

By automating access certifications, Sallie Mae eliminated the costly, time-consuming manual procedures previously used to verify and audit access controls – procedures that were also prone to error, due to the sheer magnitude of the identity data involved. The company had two full-time employees people whose sole job was to compile the access privileges of thousands of employees into spreadsheets and route them to business managers for review. Some business managers were being asked to review and validate access data in spreadsheets with more than 3,000 entries.

Just six months into the IdentityIQ implementation, Sallie Mae had automated quarterly access certifications for 52 applications and completely eliminated the need for the time-consuming spreadsheets and cumbersome process of manual review.

Instituting role-based access control

A second goal of the IdentityIQ project was to reduce the high costs associated with IT compliance. An important component of meeting this goal was implementing role-based access control to streamline user administration and create compliance efficiencies. The company used IdentityIQ to create a centrally defined role-based access control process and standardize access privileges associated with specific job functions.

Role-based access control makes it possible to manage access by developing business roles that define and standardize associations between users and their underlying access privileges. This dramatically simplifies and cuts the cost of user administration, because managers are working with a finite set of defined roles rather than an infinite number of individual users, and because the roles are defined using quickly and readily understood business language rather than arcane IT terms.

In addition to simplifying user administration, role-based access control makes compliance more efficient. It reduces the number of access review decisions that are required for compliance by aggregating entitlements, rather than requiring them to be handled individually. It also makes it easier to define and enforce business policies. Role-based access control also generally improves oversight, for greater accountability and transparency, and lowers the costs associated with audits.

Incorporating risk management

A third goal of the IdentityIQ project was to enhance Sallie Mae's data protection processes and enable the company to manage operational risk more proactively. IdentityIQ allows the company to better assess the risk associated with user access rights in order to identify and monitor high-risk user populations.

As part of this risk-based approach, and with the goal of having an immediate financial impact with the IdentityIQ project, SailPoint focused the beginning stages of the implementation on employees who service loans because of their level of access privileges to very sensitive data and applications. SailPoint performed an analysis of all sensitive system-user access data; categorized each system based on quality of identity information, access rights, and ease of extracting the

"Compliance is a never-ending chore. By using IdentityIQ to automate it, we are saving a significant amount of time and money – and improving accuracy."

Jerry Archer, CISO, Sallie Mae

data; and prioritized this list based on perceived financial risk, number of users, and quality of data. With this information, Sallie Mae could immediately identify which systems would deliver the best return for the least investment.

Strategically, automating the access certification processes for this group immediately eliminated a portion of the funds Sallie Mae was spending on FISMA compliance and helped secure funding for the rest of the project. The project team then broadened their focus and began automating the access certification processes for the rest of the company's employees, contractors and third parties.

Promoting cross-regulatory efficiencies

In order to maximize compliance efficiencies, Sallie Mae needed to comply with multiple regulations using one common approach. Its most pressing burden was associated with FISMA compliance, but it still also had to deal with other regulations such as SOX and PCI. The company had been spending significant time, effort and money on one-off compliance scenarios, and the time had come to consolidate those efforts in the interest of increasing efficiency and reducing costs.

By using IdentityIQ to automate the processes associated with identity management across all of its compliance efforts, Sallie Mae has been able to realize new levels of efficiency and cost savings, including a 90% reduction in time spent on access certification review. The new automated identity governance process that it instituted with IdentityIQ has created compliance efficiencies not just for the area of greatest immediate need (FISMA), but also for other regulatory requirements.

Providing better access visibility

As a result of the IdentityIQ project, Sallie Mae is enjoying a much-needed level of visibility into user access privileges. The company now has within IdentityIQ a single, accurate repository for identities, roles, and entitlements, instead of multiple sources of identity data associated with dozens of different applications. Having a single source of identity data makes it possible to aggregate accounts for greater visibility, and to readily identify and monitor all accounts associated with users who have the highest access levels.

Lessons learned

Sallie Mae's IdentityIQ deployment revealed several important lessons for a smooth, successful implementation of a program aimed at ensuring – and reducing the cost of – regulatory compliance.

Engage stakeholders early

Successfully undertaking the complete re-architecting of an organization's approach to compliance requires strong support from stakeholders, including business managers, application owners and administrators, and compliance teams within the company. Starting from the earliest planning stages, ensure that these stakeholders have a shared vision of what the project will accomplish and a clear sense of the part they will play, including an understanding of the time commitment that will be required.

Clearly scope the project

Knowing at the outset what applications and processes will be affected, and planning accordingly, will enable a smooth deployment. Scope your project by identifying all the key applications and their corresponding entitlements, and by identifying all the processes that need to be managed. For example, think beyond the typical activities associated with people joining, leaving, and moving around within the company, and consider whether you require other processes, such as improved automatic termination reports.

Leverage enterprise roles when possible

Enterprise roles can be leveraged across all major identity and access program components, including user provisioning, access requests, and access certification. Deploying them early in the process can simplify the implementation of all these components and reduce the risk of future rework. To smooth the path, be sure the deployment team includes someone who has successfully deployed enterprise roles in the past.

Achieve quick wins

When dealing with a multi-year, multi-phase program, aim for immediate results wherever possible. This is critical to keeping the momentum of the program going over time. At the same time, be sure to allow sufficient time to train the user community to support getting good results as quickly as possible.

SailPoint
MANAGING THE BUSINESS OF IDENTITY

Featured SailPoint Capabilities

SailPoint IdentityIQ enables organizations to align access privileges with job responsibilities and to ensure that user access conforms to business and compliance policy. Its automated role mining and modeling approach streamlines the process of defining roles while its adaptive role model allows organizations to more easily model their unique business environments.

FEATURE	FUNCTION
Data Aggregation and Correlation	Creates a single repository of user and access information by extracting data from authoritative sources, resolving data inconsistencies, and creating a single enterprise-wide view into identity data across all relevant systems.
Consolidated Access Certification Reporting	Centralizes access data, including entitlements, roles, and policy violations, across the organization and formats it into easy-to-read certification reports.
Automated Certification Workflow	Automates certification routing, notification, and escalations; the deletion or reassignment of certifications; and the ability to define challenge and remediation points.
Automated Role Creation	Automates role design via top-down role modeling and IT role mining.
Role Lifecycle Management	Manages the definition, maintenance, and retirement process for roles with automated workflows and change control.
Risk-Based Approach	Highlights key identity risk factors for users across the enterprise to focus and prioritize compliance efforts.
Business-Oriented Certification Process	Enables organization to distribute certification decisions to business users by simplifying the presentation of complex IT access data.
Closed-Loop Remediation	Ensures continuous compliance by sending automatic revocation requests to an automated or manual user provisioning system and validating that changes occurred.
Risk-Aware Certifications	Elevate identity risk scores for users who have not had timely certification reviews.

Managing the business of identity for the world's largest organizations

SailPoint, the industry leader in identity and access management, empowers the world's largest organizations to accelerate business performance, mitigate risk, reduce IT costs and ensure compliance. The company's innovative on-premises and SaaS IAM solutions provide superior visibility into and control over user access to sensitive applications and data, regardless of where they reside. SailPoint's product suite provides customers a unified solution for compliance, user provisioning, access management, and identity intelligence — all based on an integrated governance model. Founded in 2005, the company is headquartered in Austin, Texas, and has offices in Germany, Great Britain, Singapore, India, Israel and the Netherlands.

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.