SailPoint
MANAGING THE BUSINESS OF IDENTITY

Customer Successes

CASE STUDIES

See how SailPoint helps organizations around the globe.

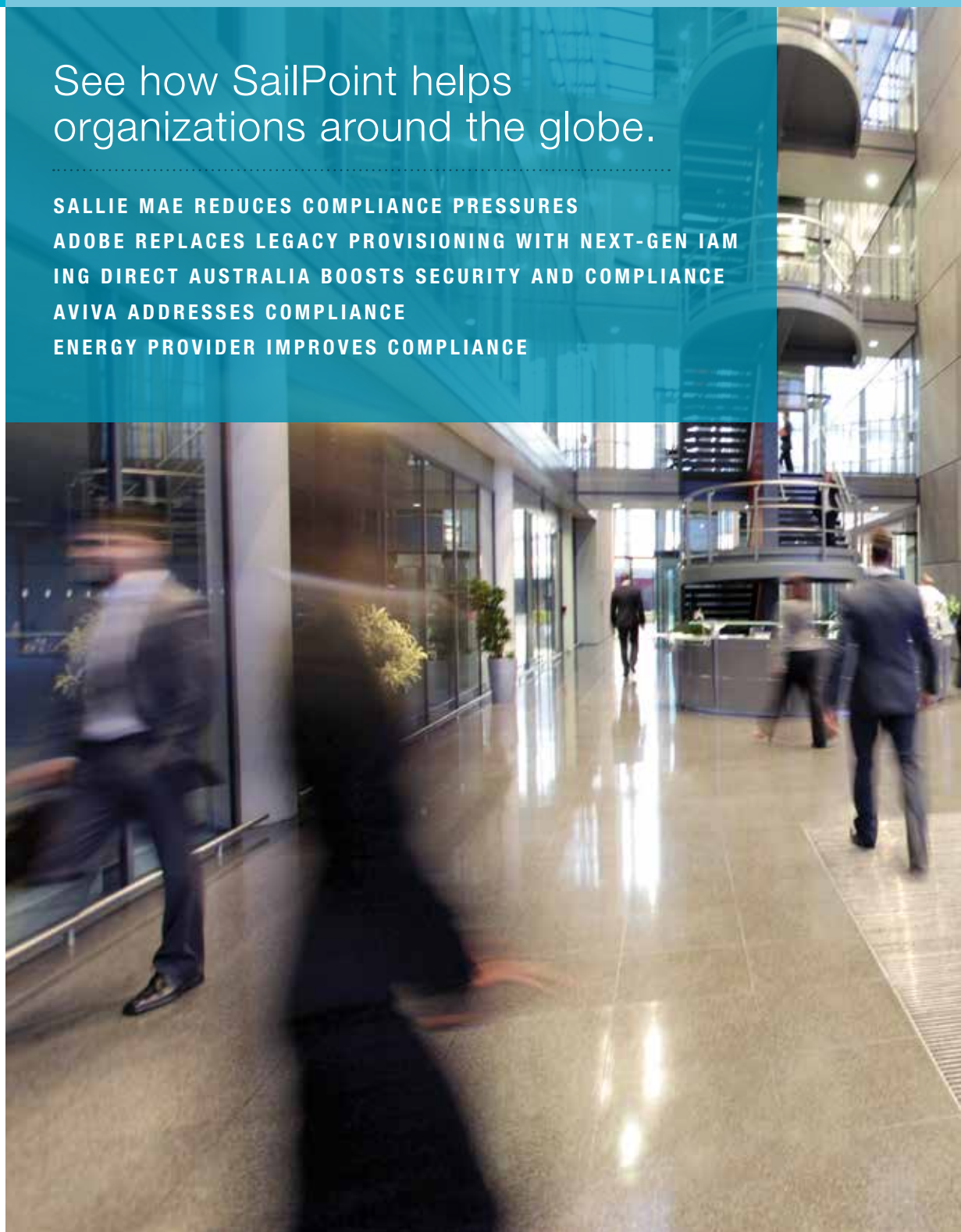
SALLIE MAE REDUCES COMPLIANCE PRESSURES

ADOBE REPLACES LEGACY PROVISIONING WITH NEXT-GEN IAM

ING DIRECT AUSTRALIA BOOSTS SECURITY AND COMPLIANCE

AVIVA ADDRESSES COMPLIANCE

ENERGY PROVIDER IMPROVES COMPLIANCE



SailPoint
MANAGING THE BUSINESS OF IDENTITY

Sallie Mae reduces compliance pressures with identity governance.

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.

"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

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; and
- Pave the way for self-service access request capabilities.

Incorporating risk management

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.

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.

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 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.

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.

SailPoint
MANAGING THE BUSINESS OF IDENTITY

Adobe transitions legacy provisioning to next-generation identity management.

OVERVIEW

Adobe is changing the world through digital experiences. The company harnesses its creative DNA to not only enable the creation of beautiful and powerful images, videos, and apps, but also to reinvent how companies interact with their customers across every digital channel and screen.

CHALLENGE

When the provider of Adobe's previous user provisioning solution announced that it would no longer support that solution, Adobe had to find a new solution that would meet all the company's provisioning needs and enable a smooth, easy transition.

SOLUTION

SailPoint IdentityIQ is a complete identity and access management solution that not only meets all the essential provisioning requirements that Adobe's previous solution met, as well as providing identity governance capabilities for additional business value.

"IdentityIQ really brings everything under one umbrella. It provides a true meta-directory of all the Adobe systems out there, so that if we add access data from any system to the identity queue, we automatically become aware of that access. We didn't have that with Sun, but the SailPoint solution is expressly designed for it"
Steve Lavigne, Manager of IT Client Services & Engineering, Adobe, Inc

When Adobe found itself facing the end-of-life of Sun Identity Manager, the company sought a new solution to meet its immediate provisioning needs and to build upon to meet future requirements.

Working with systems integrator Qubera Solutions, Adobe identified SailPoint IdentityIQ as the ideal choice to replace Sun Identity Manager. Because the SailPoint product architects had developed the core Sun technology, Adobe was confident that SailPoint was familiar with what Adobe was already doing for provisioning. But beyond that, the SailPoint team had built IdentityIQ from the ground up to deliver even more-extensive capabilities than the Sun product and to deliver a more comprehensive solution than other companies could.

Adobe was also pleased to learn that SailPoint's roadmap for future development dovetailed perfectly with Adobe's long-term vision, for provisioning in particular, and identity and access management in general. They were further persuaded by the flexibility that SailPoint offered in how to deploy IdentityIQ — from a gradual phased-in transition of the new capabilities, to an all-at-once "light switch" change.

As a result of its deployment of IdentityIQ, Adobe is able to:

- Provision user access to applications and systems for thousands of employees, clients and others who need it;
- Meet all essential user provisioning requirements with one solution;
- Plan for expansion into IdentityIQ capabilities beyond provisioning; and
- Effect a smooth, uninterrupted technology transition.

Reliable, secure access for thousands of users

Adobe is using IdentityIQ to provision access to 12 applications for 16,000 employees, contractors and vendors around the world. SailPoint provides the company with a user-driven, intuitive approach to requesting and initiating changes to access and, at the same time, provides the flexibility to provision changes in the most efficient and cost-effective way possible.

With IdentityIQ, instead of going through IT, users request access within a simple, business-friendly user interface from

which they can select the entitlements they need to do their jobs, view their current access privileges and check the status of their requests. IdentityIQ automates many routine tasks associated with fulfilling their requests. This helps control the cost of managing access in two ways: first, by enabling changes to happen more quickly and second, by minimizing the time IT is required to spend on repetitive processes associated with those changes. The solution also uses direct connections to target systems to speed delivery of requested access.

Complete provisioning functionality in one solution

IdentityIQ addresses the entire spectrum of provisioning functions, providing Adobe with one solution to take care of everything from access requests to access changes to password resets, and to manage the entire user lifecycle over time.

As with requests for new access or access changes, password resets are user-driven. IdentityIQ's intuitive user interface provides an easy way to request, manage and reset passwords, all of which can be done without burdening the IT organization. IdentityIQ automatically applies password policy to requests for passwords or password resets and synchronizes password changes with target systems. IT administrators can use that same interface to initiate password resets when circumstances warrant.

IdentityIQ provides significant flexibility in the provisioning process, allowing provisioning activities to be initiated by the users themselves, or by IT, or even by automated rules based on circumstances throughout the provisioning lifecycle. For example, if an employee is promoted to a new position, IdentityIQ can — based on policies put into place at implementation of the solution — automatically trigger the process for provisioning access to the resources appropriate to that position (and deprovisioning access to resources that are no longer appropriate).

This considerably reduces IT's burden for change management and contributes to consistent, accurate application of policy, which is invaluable in maintaining security and compliance.

Identity governance: Beyond provisioning

According to Lavigne, adopting role-based access control is one of several next steps that Adobe is looking at as the company expands its use of IdentityIQ to include capabilities beyond provisioning. "IdentityIQ capabilities like roles and access certification provide us a formal way of consistently removing access when someone leaves their job," explains Steve Lavigne, Manager of IT Client Services & Engineering at Adobe.

IdentityIQ's common governance platform is essential to bringing provisioning, roles and all the other major aspects of identity and access management together in one place. That platform will make it possible for Adobe to centralize all its identity data and business policies, model roles and build a single framework to support identity-related business processes.

Broad flexibility in deployment

Many companies moving from a legacy provisioning system to IdentityIQ elect to do so with a phased approach in order to immediately begin reaping benefits from the new solution while extracting as much benefit as possible from their existing one. However, Adobe pursued a different approach that it felt better suited the company's business processes.

"We concluded that in our case, it would be better to do a one-time change rather than a staggered or phased rollout," says Lavigne. "And with IdentityIQ, we had that flexibility." Lavigne likened Adobe's process to flipping a light switch and having everything come on at once. He emphasized that it's not the right approach for every company, but that it can work well for a company whose deployment schedule allows for fully planning and testing at all levels before going live.

Because IdentityIQ is designed to be easy to deploy using out-of-the-box interfaces and well-defined business processes, Adobe was able to make the transition from their previous system without extensive custom development, saving both time and money. The Adobe and Qubera Solutions deployment team were able to have the new system up and running in a matter of months, rather than laboring through the one- to two-year deployment turnaround that's typical of many identity and access management systems.

SailPoint
MANAGING THE BUSINESS OF IDENTITY

ING DIRECT Australia effectively meets compliance and security demands with governance-based identity and access management.

OVERVIEW

ING DIRECT is the world's leading direct savings bank and is a subsidiary of ING Group, holding a banking licence in Australia. The company pioneered online banking in Australia and is now the country's fifth largest home lender with billions of dollars in deposits and mortgages. In today's dynamic regulatory environment, responding to new and changing compliance regulations and expectations remains a high priority for the company.

CHALLENGE

As part of its ongoing efforts to maintain a sufficient level of governance, risk management and compliance (GRC), ING DIRECT Australia needed to improve its user access controls. To this end, it created an Access Control Framework outlining how the bank would manage and control access to its information resources, applications, and systems. The bank also needed an identity and access management toolset to support implementation of the Framework.

SOLUTION

With SailPoint IdentityIQ, ING DIRECT Australia was able to streamline complex identity and access management compliance processes, and automate a number of related activities, resulting in greater efficiency and improved quality and management of access controls.

ING DIRECT is always exploring innovative ways to reduce complexity, improve the effectiveness of core processes and optimize how it operates. A prime example is its proactive approach to strategic identity and access management (IAM). To ensure its operational environments are secure and robust (which has a direct impact on customer experience and thus brand reputation) and that it manages its IT risks effectively to achieve compliance, the bank chose to deploy SailPoint's next-generation identity and access management solution, IdentityIQ.

Within 90 days of the IdentityIQ project commencing, ING DIRECT Australia had implemented an IAM system that has enabled it to:

- Unify and consistently enforce access control-related business policies and processes to better manage risk;
- Apply preventative and detective controls to streamline identity-related compliance and audit activities;
- Automate cumbersome and error-prone manual processes for user access reviews;
- Identify and correct separation-of-duty (SoD) violations as part of the user access review process;
- Gain visibility into user access entitlements and privileges; and
- Improve the effort associated with executing a certification cycle by 98%, from 184 hours and two staff members to 4 hours and one staff member.

Strengthening user access controls

Like all Australian banks, ING DIRECT Australia is regulated by the Australian Prudential Regulatory Authority (APRA) and must comply with industry regulations including Basel II and Basel III. Also, since parent ING Group is a Dutch and US public company, it must be fully compliant with the rigors of Sarbanes-Oxley legislation (SOX). At the core of these information security mandates is the notion of access rights, that is, knowing "who has access to what," in particular for critical applications and sensitive customer information, and aligning access with defined internal controls.

Historically, ING DIRECT Australia assigned access rights to its applications and systems using a group and profile-based approach. However, a formal framework for the definition and maintenance of roles, groups and profiles had not been defined and documented. This impacted the bank's ability to readily assess the appropriateness of access rights to applications and systems based on users' job functions and responsibilities.

Proactive risk management and compliance

The bank's IT Security and Information Risk Management teams are responsible for information technology risk management and compliance across the organization. To satisfy both regulatory and minimum standards of access control (as defined by the bank), the teams crafted an Access Control Framework (ACF) outlining how the bank would manage and control access to its information resources, applications and systems.

A key component in the overall project was an identity and access management tool that would facilitate the automation aspect of the framework, starting with user access reviews and identity analytics and governance. Specifically, the bank identified the following business requirements that needed to be addressed by such a tool:

- Improve the efficiency of requesting and revoking access;
- Satisfy regulatory and compliance control requirements;
- Implement a role-based access request, review and control tool to manage user access across the organization, model business roles and associated system permissions, trigger manual provisioning activities and monitor and certify access initially for 30 key applications and systems;
- Complete user access reviews/entitlement certifications for the 30 in scope systems; and,
- Provide automated workflows for access request management based on the current manual access request system.

Control and visibility

With SailPoint IdentityIQ, the bank's goal was to automate and streamline the overall user access review process. In the first phase of implementation, IdentityIQ was installed in one development environment and performed the necessary configurations to demonstrate functionality for a single highly sensitive custom application. The project team began by importing user access data into IdentityIQ, and interrogating users and their entitlements in order to run a user and entitlement re-certification with supporting workflows. Following the success of this proof of concept (POC), IdentityIQ was expanded to 30 applications (in development, quality assurance and production).

Critical to the success of the project was the mapping of users to positions and identifying appropriate profiles and permissions for each. During implementation, it became apparent that the detailed technical roles and SoD policies previously defined by the bank were too restrictive and needed to be amended. As testimony to IdentityIQ's flexibility and ease of use, the bank was able to revise them, with little external assistance, in under four weeks.

Empowerment for the business users

Once the bank had cleansed its data and automated key processes, it was able to further streamline the access certification process by enabling business managers to more efficiently perform user access reviews. Line managers and applications owners are accountable for verifying whether their staff and/or privileged users have the right level of access. This allows them to view the actual access people have and address remediation of access if need be with ease and consistency.

ING DIRECT end users, responsible for performing user access reviews, have provided feedback that the IdentityIQ tool is simple to use and that reviews can be undertaken quickly. The information presented is clear and has the granularity to enable a reviewer to understand the level of access an individual has, prior to making a decision to approve or reject access. In some cases, the information presented to the asset owner also helped to identify segregation of duty rules and subsequent application profile changes to clear the conflicts

Simplified implementation and reduced costs for fast business value

Within 90 days, ING DIRECT Australia had set up core infrastructure and launched a fully automated user access certification process for 30 critical applications and 1200 active users.

SailPoint
MANAGING THE BUSINESS OF IDENTITY

Aviva addresses compliance challenges with identity governance.

OVERVIEW

Aviva is a highly regulated, global business with strong market positions in the UK, where it is based, and across Europe, Asia and North America. With a market capitalization of £11.2bn and £379bn under management, it is the largest insurance company in the UK and the sixth largest in the world.

CHALLENGE

Aviva needed to increase the effectiveness of, and eliminate inefficiencies in, its regulatory compliance efforts. To do this, the company needed an identity governance solution to automate access certifications, provide consistent controls across multiple locations, and enable centralized visibility into user access privileges.

SOLUTION

SBy implementing SailPoint IdentityIQ, Aviva has been able to meet its goal of centralized, automated access certifications and enterprise-wide access visibility. Moreover, with SailPoint the company was able to roll out a fully-operational solution across five countries and 8,000 users in less than six months.

"With SailPoint IdentityIQ, we were able to deliver a fully operational identity governance solution across five countries in less than six months."
Group Business Protection Director, Aviva

Aviva, the largest insurance company in the United Kingdom and the sixth largest in the world, has 53 million customers and 46,000 employees in 28 countries. Its size, distributed operations, and traditionally localized approach to operations posed significant challenges for Aviva in its ongoing efforts to comply with government and industry regulations. For example, as a member of the New York Stock Exchange, the company is required to demonstrate compliance with components of Sarbanes-Oxley (SOX) that govern information security. To help ensure its continuing ability to meet this requirement — as well as meet the information-integrity demands of a multitude of other regulations worldwide — Aviva established a common identity management approach to secure critical applications and data across its operations.

In order to reduce compliance and security risk, the company first needed to implement a solution that would allow it to gain enterprise-wide visibility into identity and access data and consistently certify worker access privileges across the enterprise. This process would help Aviva achieve its other primary goal of eliminating separation-of-duty (SoD) policy violations resulting from toxic combinations of access privileges among users. It would also address the problem of privileged users having inappropriate levels of access to resources. In addition to achieving these goals, Aviva wanted to eliminate costs and inefficiencies historically associated with its manual compliance processes.

Aviva chose SailPoint IdentityIQ, an automated identity governance solution, to establish consistent, centralized access controls, provide enterprise-wide visibility into identity and access data, and automate access certifications and SoD policy enforcement. The company initially implemented the solution in five countries across three continents (Canada, England, India, Ireland, and the United States) focusing on certifying users, identifying SoD issues and establishing consistent role definitions enterprise-wide. This set the stage for Aviva to ultimately move to role-based certifications in the future, speeding and simplifying the review process.

Since deploying IdentityIQ, Aviva has been able to:

- Improve the accuracy and efficiency of access certifications;
- Establish and meet specific audit benchmarks;
- Increase awareness and participation within business units;
- Improve transparency and efficiencies across all organization levels; and
- Lower the overall cost of IT compliance and decrease audit overhead.

Gaining visibility into user access

Some of Aviva's greatest compliance challenges stemmed from the company's operation of remote business units around the world, most of which had become part of the company through acquisition. As a result, many of the business units had their own unique applications, identity infrastructure, and authoritative data sources. The scope of the problem was significant: the company's IdentityIQ project, which covered five of the 28 countries where Aviva operates, involved 8,000 users with 200,000 entitlements, 100 applications, and 12 authoritative sources of user identity data.

With IdentityIQ, Aviva was able to easily collect and correlate identity data from 100 target applications and 12 HR databases, relying on IdentityIQ's unique out-of-the-box connectors to rapidly import data into a central identity warehouse from a wide variety of systems. For Aviva, this represented a significant shift toward a single, consistent "source of truth" across operations. The resulting access visibility was the first step in Aviva's long-term plan for identity governance.

Improving access certification

Once Aviva established a centralized view of access, the company's next step was to use IdentityIQ to automate access certifications. This was a logical progression, moving from seeing who has access to determining whether they should have it — i.e., establishing when access is or isn't appropriate, and providing remediation when it's not.

Aviva's program established two points of certification to help ensure security and compliance. Access privileges were first reviewed by line managers and then by system owners who manage applications and other resources. (Aviva policy required annual review by line managers and bi-annual review by system owners.) As part of the process of certifying access privileges for the 8,000 users in the initial IdentityIQ project, line managers and system owners reviewed over 200,000 entitlements.

IdentityIQ's automated certification capabilities were critical to completing the access reviews in a timely manner in order to meet Aviva's SOX compliance deadline. Prior to implementing IdentityIQ, line managers manually reviewed entitlements in spreadsheets, which proved to be a slow, costly, and error-prone process. With IdentityIQ, however, Aviva was able to automate all required access certification tasks, including formatting access data into easy-to-read reports for business users, routing reports to line managers and system owners or review, tracking progress and actions, and producing reports for auditors.

Identifying and eliminating risk

In any IT environment, the greatest risk for violations of internal policies and external regulations often lies in the failure to detect and revoke inappropriate access. From orphan accounts where terminated employees continue to have access rights, to toxic combinations of access privileges that violate SoD policies and regulatory requirements, to excessive access being awarded to privileged users, the risk of violation is always present. One of the goals of the Aviva project was to minimize exposure by accurately identifying and then quickly dealing with these security and compliance risks.

Before implementing IdentityIQ, Aviva's manual access certification processes typically resulted in 3-5% of the entitlements reviewed being revoked because they reflected inappropriate levels of access to resources. This figure increased to 10-12% when the company instituted an automated approach with IdentityIQ. In the first round of reviews by line managers, the company identified more than 22,000 inappropriate entitlements. As a result, the access privileges associated with them were revoked, dramatically reducing the incidence of excess privileges and toxic access combinations in the company. The experience provided tangible evidence that the automated processes were enabling reviewers to more effectively identify and remediate inappropriate access.

Lowering the cost of compliance

Because of the the rapid deployment of a fully operational identity governance solution in place — IdentityIQ was deployed in less than six months — Aviva began seeing a return on its IdentityIQ investment very quickly. The company benefitted almost immediately by replacing slow, costly and error-prone manual processes with a more efficient and accurate automated process.

As Aviva expands the IdentityIQ implementation, the company expects to continue to improve compliance through greater accuracy of access certifications, at a lower cost, thanks to automation. The new certification process, once it's fully deployed across the entire company, will save the equivalent of 50 full-time employees annually in testing and documentation alone. Lower audit overhead is also anticipated, because all the information that auditors need is automatically tracked and stored in a centralized secure repository, where it's readily available to them. Auditors no longer have to test every individual control in every location, because a consistent set of controls applies across the entire enterprise.

SailPoint
MANAGING THE BUSINESS OF IDENTITY

Energy provider improves compliance with identity governance.

OVERVIEW

This $10 billion gas and electric utilities provider serves more than five million metered customers in six states and employs more than 9,000 people worldwide. The company faces a variety of regulatory pressures, including the need to comply with industry-specific NERC CIP reliability standards, Sarbanes-Oxley requirements for public-company accountability and other regulatory demands.

CHALLENGE

The company's constant challenge is to improve its compliance performance while keeping costs under control.

SOLUTION

The company selected SailPoint IdentityIQ to deliver integrated identity governance to its existing identity infrastructure. With the preventive and detective controls, increased visibility, and repeatable compliance processes provided by IdentityIQ, the company is now able to easily and cost-efficiently identify and revoke inappropriate access, detect and remediate policy violations, and eliminate high-risk accounts.

"With IdentityIQ, we were able to reduce the certification workload on IT staff, freeing them up to focus on their daily jobs. Even better, IdentityIQ has made certs a less error-prone, more defined process."
Information Security Manager, Energy Delivery Company

As a member of one of the most highly-regulated industries in the world, this Fortune 300 energy provider is no stranger to the demands of regulatory compliance. Faced with compliance and audit requirements from both Sarbanes-Oxley (SOX) and the North American Electric Reliability Corporation (NERC), the company embarked on an initiative to improve its compliance performance while streamlining and simplifying labor-intensive compliance processes. Its goals were to demonstrate compliance and effective risk management, while at the same time reducing costs and lessening the burden on IT.

One of the most pressing requirements mandated by SOX and NERC Critical Infrastructure Protection (CIP) regulations is the need to implement strong controls over access to critical IT assets. For this reason, the company initiated a project to focus on identity and access governance, with three key goals: to centralize visibility over user access privileges across enterprise resources; to implement role-based access control; and to align IT and business managers in automated processes to improve oversight and reduce risk.

Working with its strategic implementation partner, Partners Consulting Inc., the energy provider implemented an automated identity governance solution provided by SailPoint. The solution, SailPoint IdentityIQ,™ allowed the company to automate key controls over user access, to centralize visibility across the enterprise, and to implement a risk-based approach to identity management. The solution was designed to be both easy for IT to deploy and for business managers to use, and to provide quick return on investment.

Since deploying IdentityIQ, the company has been able to:

- Improve the efficiency and accuracy of access certifications;
- Automate detection and enforcement of separation-of-duty (SoD) policies;
- Simplify compliance by using roles to align access privileges with job functions;
- Quickly and easily identify and eliminate high-risk accounts; and
- Meet audit requirements with on-demand reporting.

Fast integration with critical applications

One of the key determinants for selecting SailPoint for the identity governance project was its ease of implementation and ability to quickly aggregate data from the mission-critical platforms and applications that were the focal point of

compliance. The environment included Active Directory, RACF, UNIX, Linux, and Windows platforms, and packaged applications such as SAP, as well as custom applications.

The customer particularly liked the fact that IdentityIQ was architected for fast connectivity to the SAP® environment. IdentityIQ offered superior SAP integration, with out-of-the-box connectors for quickly aggregating SAP data, support for data extraction and modeling across SAP ERP and HR, and standardized BAPI-based integration with SAP.

Centralizing data and automating certifications

Once the set of high-risk applications was identified, the project team began the process of aggregating and correlating identity and access data from the 32 critical applications into a central repository within IdentityIQ. Once the data was centralized, the team began the process of access certification and data cleanup to remove inappropriate access and to verify that user access privileges were correct and compliant.

As part of the initial data aggregation and certification phase, business and IT managers gained a comprehensive view of identity data that allowed them to identify high-risk accounts, such as orphan accounts and shared or privileged accounts. After the completion of the initial round of certifications, the company discovered that over 15% of access privileges were inappropriate or unnecessary and targeted them for remediation.

Adopting role-based access control

To further simplify and improve compliance performance, Partners Consulting worked with the project team to define and create roles using IdentityIQ's role mining and role lifecycle management capabilities. Using input from business users, business roles were developed that clearly defined the association between users and their underlying access privileges. The business roles were then associated with IT roles and mapped to the underlying access privileges required to complete specific tasks within the IT environment.

By standardizing user access privileges with business roles, the project team was able to improve the accuracy of entitlements, increase the efficiency of business users who request and certify access, and ensure that access rights adhere to the company's business and regulatory policies. The roles also allowed the company to define separation-of-duty (SoD) policy to simplify detection of toxic combinations of access privileges held by users across all 32 critical applications and platforms.

Upon completion of the first phase of role management, the company created over 100 roles and defined dozens of SoD rules that are automatically enforced by SailPoint. This effort has made it much easier for managers to monitor and enforce SoD policy going forward and to demonstrate proof of compliance to auditors.

Involving business users

One of the key goals of the project was to facilitate greater participation of business users in identity compliance processes. Before implementing SailPoint IdentityIQ, the company relied heavily on IT security personnel to conduct certifications and support SOX and NERC audits. SailPoint's business-friendly user interface, together with the creation of business-relevant roles for certifying access and detecting SoD policy violations, enables business users to help define policy, review access, and run audit reports.

"Our client had very specific business objectives they wanted to achieve around compliance," explains Jim Guinn, Executive VP of Partners Consulting. "All managers had to be able to certify and self-attest to the user access privileges held by their employees. This meant that we had to make it possible for line-of-business managers to sit down and — with little or no training — log in and certify users."

Integration with existing investments

In order to automate the fulfillment of remediations generated by IdentityIQ, the company took advantage of SailPoint's integration with Sun Identity Manager. The packaged integration with Sun enabled the company to automate its process for revoking access privileges and reduced the burden on IT staff to manually handle change requests. The closed-loop remediation provided by IdentityIQ enabled the project team to validate the status of all remediation requests, increasing accountability and control over the process.

Realizing the value of risk management

IdentityIQ's ability to implement a risk model across roles, policies, and entitlements played a key role in the selection of SailPoint for the project as the project team believed it to be a tremendous value.

SailPoint
MANAGING THE BUSINESS OF IDENTITY

Lessons Learned

After hundreds of SailPoint deployment, there are a few key lessons that are worth sharing. Here are some key lessons learned that will help achieve quick results with an early return on investment as well as ensure a smooth, successful implementation of your identity management program.

Build the team

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.

Establish a governance committee and a working group from across lines of business

To share best practices, processes, policies, and work streams. This is helpful as it allows different business units to share and leverage work and will accelerate enterprise level deployment. Establishing clear responsibilities for business units is important to maintaining that commitment throughout the project.

Engage a technical project manager

In addition to a business sponsor/program manager, there is a need for a technical project manager who understands technology, and who has depth knowledge of governance, risk management and compliance. Ideally this person should also understand your environment and be able to guide the implementation team through company standards and policies.

Engage audit and compliance

If possible engage audit to work with you as early as possible and for them to be a joint stakeholder in the program.

"Best results are achieved by taking a stepwise approach where your project is focused on the business units, departments, or applications that align with your business goals — whether they are corporate agility, operational efficiency, service-level improvement, or regulatory compliance."

Enlist support from the top

Immediate project sponsorship by group executives, CIOs, and business unit stakeholders will provide the catalyst for change that is essential to the success of any identity management project. For example, in Aviva's case, central funding and sponsorship on the part of the CFO helped the company avoid potential barriers to progress.

Define project scope

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.

Identify a specific business driver

The presence of a major business driver can help accelerate the path to progress by giving everyone from management on down a tangible reason to get onboard. A compliance deadline can serve as the pressing pain point to strong and immediate project commitment.

Remember the importance of upfront analysis

Don't jump into "just do it mode." At the same time, however, avoid analysis paralysis. Prototyping and iterative development are valuable for gathering and refining detailed requirements, and ensuring that functionality (and hence business value) is delivered as early as possible.

Rely on independent specialists

In general, SailPoint customers are not identity management software companies. By relying on SailPoint's specialized expertise, customers are able to make progress quickly and show management an early return on the company's investment in the project. And while independent expertise is important, customers have learned that engaging internal IT resources in the process and establishing their responsibilities early on is equally important.

Measure success and move ahead

Build confidence with a phased approach

The best results are achieved by taking an incremental approach to project implementation, where the focus is limited to applications that are high priorities from a compliance or operational efficiency perspective. This allows for small, quick wins to build confidence in the solution and help ensure ongoing adoption. Begin by identifying the most critical applications, users, and project tasks based on business drivers and proceed from there on a step-by-step basis to expand project scope.

Take an incremental approach to role management

Developing a role management solution does not have to take years if appropriately scoped. Roles can be rapidly developed to support compliance by aligning access privileges to user job functions within the organization and using automated tools for mining and modeling. Take an iterative approach for role management. Start with a small group or department, see what works, then use the knowledge gained to refine and expand your models, and then expand your scope to more groups.

Choose a solution that engages and empowers business users

When business users are able to perform compliance tasks without relying upon IT, there is an immediate positive effect on the efficiency and cost-effectiveness of the overall compliance effort. Find a solution that incorporates business context into the technical data so that business users are able to make more educated decisions and improve accuracy of certifications overall. Keep in mind that a solution that offers ease of use for non-technical staff can be invaluable for keeping costs down and enabling IT to focus on more strategic areas of IT rather than the menial tasks that compliance processes entail.

Clearly communicate improvements

Making sure everyone understands just how much more effective new recertification or provisioning processes are compared to previous ones can be very useful in keeping levels of project support high.

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

Customer Successes

Large U.S Commercial Bank

One of the largest U.S. commercial banking companies needed better visibility and stronger controls over user access privileges to meet the rigorous requirements of regulatory compliance, security and risk management. 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.

One of Europe's Largest Banks

Using a hosted version of SailPoint IdentityIQ, one of the world's largest banks launched a fully-automated access certification process across 87 compliance-relevant applications. The deployment included cleansing and centralizing identity data for over 145,000 users. The customer has on-demand visibility into access rights, transitioned from manual certification process for more efficient and accurate audits and ensures that access rights conform to corporate business policies.

Global Bank

One of the top 15 banks in the world is working with SailPoint to improve their compliance performance and overall risk posture. Within 60 days, SailPoint delivered an identity governance solution that allowed the bank to launch a fully-automated access certification process across 29 SOX-relevant applications. The deployment included cleansing and centralizing identity data for over 25,000 users.

Major U.S. Telco

A major U.S. telecommunications company with well over 200,000 employees is using IdentityIQ to aggregate and correlate user and account data across 150 enterprise data sources, 500,000+ entitlements and 3,000 reviewers. This customer has simplified the access review process by defining a high-level role model which incorporates business-friendly entitlement descriptions. And, they've implemented advanced policies to quickly scan and detect SoD violations between enterprise applications keeping them compliant with demanding compliance requirements.

Global Financial Services Firm

Using IdentityIQ, this leader in financial services is working with SailPoint to eliminate "toxic combinations" of access and to lower overall business risk. Their identity governance project focuses on managing identity data for thousands of enterprise applications and has aggregated over 10 million individual user entitlements. With IdentityIQ, this customer has simplified certification of multi-tiered applications and reduced 400+ target systems to 195 applications for certification and cut the extraneous certification items on these systems in half.

Software and Financial Services

A leading provider of business software and financial management solutions wanted to proactively manage the risks associated with worker access to sensitive data, strengthen its access management practices, and improve IT productivity. Within 14 weeks, SailPoint enabled the customer to cleanse the data across its most critical applications, gain a centralized view into more than 1 million entitlements, automate the access certification process and streamline the remediation process for removing inappropriate access.

Energy Utilities: Fortune 300 Energy Provider

A Fortune 300 energy provider facing compliance and audit requirements from both Sarbanes-Oxley (SOX) and the North American Electric Reliability Corporation (NERC) wanted to improve compliance performance while streamlining and simplifying labor-intensive compliance processes. The company selected SailPoint IdentityIQ, to deliver integrated identity governance to its existing identity infrastructure and is now better equipped to easily and cost-efficiently identify and revoke inappropriate access, detect and remediate policy violations, and eliminate high-risk accounts.

A Global 100 Financial Services Leader

A European-based insurance and financial services provider automated their access control review and reporting process with SailPoint. By streamlining user access reviews for more effective and sustainable compliance, they dramatically increased the accuracy of user and entitlement data and are now better equipped to meet the requirements of SOX.

"CUNA Mutual wanted to improve the accuracy and efficiency of access certification and more efficiently control the provisioning and de-provisioning processes. SailPoint IdentityIQ was the obvious choice because it delivered identity governance and provisioning capabilities in a single solution. It was also immediately evident that it would be easy for our business managers to use, and provided us insight into the risk associated with user access. Through our partnership with Logic Trends, we were able to define our identity management requirements, evaluate a number of the industry available solutions and quickly see results from a rapid first phase implementation."

Director of Information Security, CUNA Mutual

"With SailPoint IdentityIQ, we were able to deliver a fully-operational identity governance solution across five countries in less than six months."

Group Business Protection Director, Aviva

"By using roles to request, approve and certify user access privileges, BNSF will be able to simplify its user administration and compliance processes. SailPoint IdentityIQ will allow us to enforce and verify role-based access across our critical enterprise applications using a streamlined, automated approach."

Bart Boudreaux, Director, Technology Services, BNSF Railway

"SailPoint IdentityIQ will allow us to move from a manual process that provided fragmented visibility into our identity controls to a fully automated process that provides full visibility into and control over our enterprise identity data."

Global Head of Security Operations, Rabobank International

"SailPoint helps us define the connection between user access, financial control and intellectual property protection. Their risk-aware approach focuses on the relative risks associated with user access within our business"

Russ Finney, Vice President of U.S. Information Systems Operations for Tokyo Electron, U.S. Holdings

SailPoint
MANAGING THE BUSINESS OF IDENTITY

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 global 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.