CUSTOMER
SUCCESS STORY

Adinsec
Identity Architects

SailPoint
MANAGING THE BUSINESS OF IDENTITY

AXA Improves Identity Governance and Administration with SailPoint IdentityIQ

FINANCIAL SERVICES

OVERVIEW

AXA is a leading financial protection organization, and the number-one insurance brand in the world. AXA serves 102 million customers in 56 countries with property and casualty insurance and health coverage, as well as financial protection and asset management services.

CHALLENGE

AXA Belgium needed an automated identity and access management (IAM) solution to serve the dual purpose of simplifying access requests for external customers and improving access processes for internal teams.

SOLUTION

SailPoint IdentityIQ is an agile solution for identity and access management that simplifies access requests for corporate customers and also makes managing access rights easier and more secure for internal teams.

Faced with increasing risk and costs associated with manually managing external and internal access to business applications, AXA Belgium made the decision to move to a centralized, automated system for identity governance and administration (IGA). The company needed a solution that would not only improve internal access and certification processes, but also empower external customers to securely manage their own access to insurance policy and claims information.

AXA began the search for the ideal IAM solution with a risk assessment of its current environment, conducted by Adinsec Identity Architects, which identified areas for improvement in managing access privileges. Next, AXA elected to begin with a project to implement access and role management for external users among its corporate customers. Working with Adinsec, AXA chose SailPoint for the project.

AXA's decision was based largely on SailPoint IdentityIQ's capability of supporting agile implementation methods in several areas. This includes the ability to manage access to business objects (in this case, insurance policies) and not just to IT systems, as well as the flexibility to support multiple languages, since Belgians are typically multilingual. SailPoint was also willing to go above and beyond its standard language support, which already covered the French, German and English languages required, and add support for Dutch (Flemish) as well.

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

- Empower corporate customers to manage their own access
- Exert secure control over internal and external access rights
- Automate and streamline access certifications for business users
- Scale easily to handle growing numbers of objects and applications

"With SailPoint IdentityIQ, we now have an established set of processes in place to manage identities and access rights as we add new internal users, new applications, and as we invite external users into our application."

Security Architect, AXA Belgium

Putting customers first: Simplified access requests for policyholders

It's typical for an organization to launch an IAM solution internally before rolling it out to external users. In AXA Belgium's case, however, the benefits that would come with deploying SailPoint IdentityIQ externally were so compelling, the company embarked first on an IGA project to simplify access requests for corporate customers.

Focusing specifically on AXA Corporate Customers, the SailPoint solution enables AXA to delegate administration of insurance policies to the companies themselves. Instead of having to engage AXA to define access policies, authorize access rights, recertify and decertify access, and handle other related processes, the companies are able to do these tasks themselves using SailPoint IdentityIQ. The shift benefits customers by empowering them to manage their own access needs, and it benefits AXA by reducing the operational load associated with managing access for customers.

"The customer doesn't see the additional responsibility as a burden, but as a benefit, because it gives them more direct control over the process," says Désiré Noël, CEO of Adinsec. "And at the same time, there's less need for manpower on the AXA side."

IdentityIQ delivers complete user lifecycle management capabilities to AXA customers, enabling them to easily assign roles and privileges in accordance with their specific needs. Determinations about who should be granted access to what lie entirely with the HR department of the insured company, and IdentityIQ provides a straightforward, simplified process for the customer to align access privileges with job responsibilities.

More efficient, effective control over internal access rights

Turning to AXA Belgium's internal operations, the challenge was how to move from an ad hoc manual process to an automated standardized process. One of the goals of the internal deployment was to be able to ensure that user populations do not have any more access rights to critical applications than what is necessary to perform their jobs. AXA's first step toward this end was standardizing on IdentityIQ as a centralized system of access control to replace the many silo'ed controls that had historically characterized the company's IT environment.

"We wanted to deploy a centralized solution that would allow us more visibility," says a security architect at AXA Belgium. The governance-based IdentityIQ solution provides visibility into access rights throughout the entire organization. It also serves as the foundation for a "Joiner, Mover, Leaver" program for efficiently requesting and revoking access rights throughout the user lifecycle. Having a formal program in place limits risks associated with former employees, brokers and others still having access rights to which they're no longer entitled after their relationship with the company has ended. It also helps ensure that every time an employee's role within the company changes, his or her access rights change accordingly, to avoid an inappropriate accumulation of privileges over time.

Improved access certifications and other processes for business users

One of the greatest IAM challenges for AXA was in access certifications. The company's existing IAM model was based on technical terminology, which made it difficult for non-technical, business users to make informed decisions when asked to grant access requests or to certify users' access.

"Business users need to have clear insight into current access rights, but that's difficult if they're asked to certify access using unfamiliar, technical terminology," says a security architect at AXA Belgium. "Business users need to be able to manage access using everyday business terminology."

In addition to being difficult to use, AXA's existing IAM model was inefficient. Managers certified access using a slow, spreadsheet-based manual process. There was also no single, consistent, standardized way to handle access requests and revocations.

IdentityIQ addresses all of these issues. It's an automated, governance-based tool that automates and standardizes access management processes for AXA, speeding access certifications and access request workflows. And because IdentityIQ's access management model is based on business terminology, it enables managers to quickly and accurately recertify rights for the company's most critical applications.

A standardized, scalable solution for effectively managing access

IdentityIQ is enabling AXA Belgium to meet a number of business goals; at the same time, the solution is addressing the IT team's own specific set of objectives. The solution has enabled IT to standardize and simplify the IAM architecture landscape, eliminating multiple processes and technologies in favor of one enterprise-wide solution.

IT also needed the IAM solution to be highly available and scalable, given the growth in the number of users and managed objects. For example, just the initial external project alone has already placed 600,000 objects under management. IdentityIQ provides the scalability to ensure that the solution is highly available regardless of how far across – and beyond – the enterprise it extends.

Finally, to streamline IT operations associated with identity management, IdentityIQ makes it easy to identify and eliminate roles that are no longer used, and to identify and decommission application administration components that are no longer needed.

Lessons Learned

AXA Belgium's deployment of IdentityIQ provided several lessons about how to ensure a successful deployment.

Enlist management support

Regardless of what type of IAM solution – or which specific solution – a company chooses, high-level management support is essential to getting the project off the ground and seeing it through. In AXA Belgium's case, Adinsec had an ongoing trusted relationship with a C-level executive who provided the needed executive support to make this project happen.

Take a phased approach to deployment

By rolling out an IAM solution in waves, as AXA did, a company can begin to determine soon in the process how well the solution is working and where adjustments may be needed – rather than waiting a year or longer to complete the rollout and then assess its effectiveness across the entire enterprise. AXA elected to deploy their solution first to customers before bringing it to internal operations. The internal deployment was also phased, with implementation taking place in one business unit at a time.

Demonstrate results early and often

A related advantage with an agile deployment is the ability to show results quickly. "We delivered something every week, even if it was something that was still in progress, and we also provided an hour-long demo to the business every month," says Noël. "The fact that this can be done with SailPoint IdentityIQ is definitely a plus for the product."

Continually delivering demonstrable benefits also helps get other business units onboard for future rollouts. The AXA Belgium project started very narrowly with one corporate customer application, but the positive results have resulted in other business units also wanting IdentityIQ deployments.

SailPoint
MANAGING THE BUSINESS OF IDENTITY

Featured SailPoint Capabilities

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

CAPABILITY	DESCRIPTION
Compliance Manager	
Access Certifications	• Automate access review cycles with flexible scheduling options • Present data in business-friendly language • Focus reviewers on exceptions and high-risk items • Track reviewer progress and actions • Enforce a closed-loop provisioning process
Audit Reporting	• Highlight effectiveness of compliance controls • Archive certification and policy violation history
Lifecycle Manager	
Self-Service Access Request	• Empower users to request and manage access using an e-commerce shopping experience • Facilitate access approvals with mobile device interface • Provide visibility to request status and process execution
Lifecycle Event Management	• Automate access changes based on HR lifecycle events (i.e., hires, transfers, terminations) • Prevent policy violations and consistently enforce the desired state • Orchestrate changes across automated and manual provisioning processes • Gain complete visibility to process execution
Governance Platform	
Identity Warehouse	• Leverage single system of record for identity data across all IAM functions and activities • Import data using out-of-the-box connectors or via flat files
Policy Model	• Define and implement detective and preventive controls with compliance, access request and provisioning policies • Proactively identify and route violations for review or immediate revocation
Role Model	• Discover business and IT roles based on identity attributes and entitlements • Provide automated role approvals, role certifications, role quality metrics and role analytics

About Adinsec

Adinsec
Identity Architects

Adinsec/Grabowsky offers large organizations in Belgium, The Netherlands and Luxembourg proven solutions for Identity Governance and Identity and Access Management and helps them to get better control over the administration of and insight into critical information security data. AdinSec works with market-leading suppliers like SailPoint to offer its customers future-proof solutions while assisting customers as well as large consulting organizations in the implementation of these solutions.

About SailPoint

As the fastest-growing, independent identity and access management (IAM) provider, SailPoint helps hundreds of 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 about SailPoint, please visit www.sailpoint.com.

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