# Insurance company improves efficiency and SOX compliance

## Speeds system-access approvals by 97% and cuts risk with standardized identity and access management workflows

**Industry:**

Insurance brokerage

**Company:**

Customer: Leading global insurance company with 40,000 employees

**Country:**

United States

**Challenge:**

To drive efficiency, simplify growth and comply with SOX regulations, a top insurance company had to automate and standardize its identity and access management (IAM) processes.

**Products & Services:**

- One Identity Manager

**“It used to take two-and-a-half months to attest access to our financial system. With Identity Manager, it takes just two days. And we complete 250,000 attestations every quarter.”**

Director,
Global Identity and Access Technologies,
Large Global Insurance Company

**97% faster** attestations on user access

**250,000** attestations per quarter

**60% fewer** help-desk calls

**99.999%** uptime

Scalable to support **100% growth**

**Improves** SOX compliance, efficiency, and user experience

To compete, insurance and risk-management firms must deliver responsive, affordable services. Doing so requires highly efficient staff, low operating costs and compliance with the Sarbanes-Oxley (SOX) Act as well as other regulations such as GDPR, the NYDFS Cybersecurity Regulation and the California Consumer Privacy Act. Meeting these requirements can be especially challenging for rapidly growing companies with geographically dispersed sites, which is exactly what happened to one of the world's largest insurance companies.

The company's leadership recognized that their disparate identity and access management (IAM) workflows jeopardized compliance and hindered efficiency. Help-desk staff manually provisioned and deprovisioned access to applications based on email requests. As a result, there were inconsistencies in who could use what. Employees often had to wait to access the digital resources they needed—and people who left the company or switched roles sometimes had access longer than they should. Creating SOX attestation reports meant tedious spreadsheet reviews. Mobile employees had to use a cumbersome portal to access applications. And any integrations with human resources (HR) systems were extremely difficult.

## A comprehensive, affordable IAM solution that can support 100% growth

To meet requirements, the company evaluated IAM offerings from One Identity, Avatier and CA—and chose One Identity Manager. It could automate employee onboarding, offboarding, attestations and self-provisioning, as well as support 100 percent growth. "One of the biggest reasons we chose One Identity Manager is that it can scale," says the Director at the insurance company. "At the time, we had 20,000 users but we knew within two years, we'd have 40,000. Also, from a cost perspective, One Identity delivers the best ROI."

Company IT staff teamed up with consultants from One Identity partner iC Consult to design and deploy the solution. Steps included connecting Identity Manager to HR systems, which contained corporatewide employee profiles and their roles. They also created automated provisioning, deprovisioning and approval workflows that are triggered by events such as a new hire, a promotion, or someone leaving the company. The engineers also configured a self-service portal for requesting access and two-factor authentication for mobile employees. "The initial setup of Identity Manager was straightforward," says the Director. "The functions really are ready to use out of the box. We didn't have to do a lot of development."

"We've **reduced help-desk calls by 60 percent** because people no longer have to contact us for access. Across our sites, people have **recouped significant time** to focus on their jobs now that we use Identity Manager."

Director,
Global Identity and Access Technologies,
Large Global Insurance Company

## Three months to deploy and 99.999% availability

Implementing the solution to all corporate sites—and training the staff to use and manage it—took less than three months. In addition, two years after the initial deployment, the company engaged One Identity Manager Professional Services to help upgrade to version 8 of Identity Manager to keep the solution current. "People praise the user interface of Identity Manager 8," the Director says. "It's also faster than our previous version and available 99.999 percent of the time."

## Real-time provisioning cuts risk and boosts compliance

With its new solution, the company has cut risk and improved SOX compliance. That's because employees' access privileges correspond with their HR profiles in real time. "We've automated all onboarding and offboarding processes using Identity Manager and a live feed from our HR database," says the Director.

## Attestations take 2 days instead of 75

It takes 97 percent less time to attest—or certify—who has access to what using One Identity Manager compared with the previous workflows because processes are automated and documented. The Director explains, "It used to take two-and-a-half months to attest access to our financial system. With Identity Manager, it takes just two days. And we complete 250,000 attestations every quarter."

## Reduces help-desk calls by 60%

Help-desk staff are more efficient and there's less risk to compliance now that access requests are centralized and automated. "We've reduced help-desk calls by 60 percent because people no longer have to contact us for access," says the Director. "Across our sites, people have recouped significant time to focus on their jobs now that we use Identity Manager."

## About One Identity

One Identity, a Quest Software business, lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of a program, enabling proper access across all user types, systems and data. Learn more at OneIdentity.com.