CASE STUDY

Proper identity and access management protects against fraud

Insurer in France implements efficient identity management, improving compliance and enabling three times faster answers to auditors' requests

Key Facts

Company
Natixis Assurances Metiers Non Vie (NAMNV)

Industry
Insurance

Country
France

Website
assurances.natixis.com

Challenges

NAMNV wanted to protect itself against internal fraud. To do that, it needed to manage its authorisation and recertification practices, and enhance reporting capabilities.

Results

The insurance provider is now able to answer audit requests three times faster to improve compliance, and it has more accurate identity access management (IAM) data to protect against fraud.

Products

Identity Manager

Password Manager

Fraud is a multi-faceted threat that is of growing concern for all businesses today.

In France, a recent survey led by leading European insurance fraud organisation Euler Hermes found that, "80 per cent of companies in France have experienced at least one instance of attempted fraud."

Companies in the insurance industry are more at risk than most, given the fact they handle masses of highly sensitive financial data. In light of this, Natixis Assurances Metiers Non Vie (NAMNV), a French insurer, wanted to minimise what it saw as its most pressing vulnerability: internal fraud, which is often enabled by weak identity and access management practices.

NAMNV is part of Natixis Assurances, itself the corporate and investment banking, insurance and financial services arm of Group BPCE, the second-largest banking group in France with more than 36 million customers. It's responsible for supporting bank advisors on insurance solutions, managing insurance contracts, and creating non-life insurance

"With One Identity Manager, any inconsistency in the workflow can be easily identified, which means we're better protected against fraud."

Adrien Bertrand, IAM Project and IT Security Manager, Natixis Assurances Metiers Non Vie (NAMNV)

solutions that are distributed across the Group BPCE network. NAMNV has more than 250 staff dedicated to bank advisor support, and around 600 additional employees across call centres in Bordeaux, dealing with admin, compliance and accounting.

NAMNV is part of Natixis Assurances, itself the corporate and investment banking, insurance and financial services arm of Group BPCE, the second-largest banking group in France with more than 36 million customers. It's responsible for supporting bank advisors on insurance solutions, managing insurance contracts, and creating non-life insurance solutions that are distributed across the Group BPCE network. NAMNV has more than 250 staff dedicated to bank advisor support, and around 600 additional employees across call centres in Bordeaux, dealing with admin, compliance and accounting.

A new identity

NAMNV's legacy approach to identity and access management (IAM) consisted of Microsoft Excel spreadsheets, which IT staff kept up to date manually. This didn't allow IT to reliably track requests and it took a week to create a single user profile. It was this set of sticking points, alongside the wider context of fraud reported in Hermes' survey, that encouraged NAMNV to move forward on its internal IAM transformation.

It identified several objectives that its new solution needed to provide. To reduce the risk of internal fraud, NAMNV wanted to track and automate its user lifecycle processes — origin, authorisation, and recertification — and implement richer management workflows. The insurer also wanted more comprehensive reports with on-demand data tracking to satisfy the frequent requests sent by internal auditors. Finally, NAMNV wanted to automate and update its processes, such as recertification, to free up the IT team by giving business managers increased visibility and control.

Next step: selecting the right solution

Having set out its requirements for the ideal IAM solution, the insurer evaluated offerings from several vendors. The One Identity solution, which included Identity Manager and Password Manager, stood out. Its architecture uses open databases, and it easily integrates with Windows virtualized environments for shorter deployment times because it doesn't need extra servers to process tasks – both important advantages for NAMNV. The solution also provides key functionalities, including request tracking, profile creation, recertifications, and full visibility on authorisations. In short, the solution promised NAMNV a more rigorous, efficient, and transparent way to manage and govern identities and access.

Capitalising on an opportunity

With the One Identity solution, NAMNV staff now have accurate detailed IAM data at their fingertips. Adrien Bertrand, IAM project manager and IT security manager at NAMNV, says, "With One Identity Manager, any inconsistency in the workflow can be easily identified, which means we're better protected against fraud."

The organisation can also answer auditor requests three times faster, with fewer people . This is down to better reporting capabilities with One Identity Manager, allowing staff to find answers on rights and access quickly and efficiently. Together, it makes for stronger compliance.

A key requirement for NAMNV was including business managers in the authorisation process. This is now possible through Identity Manager, which gives managers full visibility of their team members' access rights and the ability to manage those rights throughout a user's lifecycle. The solution has proved popular, with 100 percent of business managers adopting the solution.

Bertrand says the future-ready architecture is simple to manage: "We appreciate the fact Identity Manager works out of the box, and we love the authorisation governance it delivers. Even after integrating several apps into the solution, it remains easy to manage. It just works!"

Learn more: OneIdentity.com

The One Identity logo is a trademark of One Identity LLC and/or its affiliates. Other trademarks are property of their respective owners. Availability and terms of our solutions and services vary by region. This case study is for informational purposes only. One Identity LLC and/or its affiliates make no warranties – express or implied—in this case study.