_betasystems

INVESTITIONSBANK BERLIN

Investitionsbank
Berlin

AUDITORS 'STRONGLY RECOMMEND' AUTHORIZATION MANAGEMENT

The staff of the 'monitoring office' of Investitionsbank Berlin (IBB) used to have a very tough job. It is their responsibility to regularly check the IT authorizations of the financial service provider's 850 employees. This means that they also play a key role in ensuring that the bank meets all compliance provisions. However, given the steadily increasing number of regulations for the finance industry, manual verification is a time-consuming and error-prone task. What further complicated matters was that numerous IT systems of IBB were not connected to a central identity access management (IAM) system. For these reasons, IBB introduced the Beta Systems GARANCY Suite in the fall of 2016. The resulting improvements regarding the quality and speed of authorization monitoring speak for themselves.

This was not the first time for IBB to address the topic of IAM. Any large company with many employees, who use dozens of systems, must ensure that each person can access the IT systems – and only those systems – needed to perform their job. In 2000, the bank purchased an IAM system of another provider, which managed access rights via the Windows Active Directory service (as well as the Novell-based eDirectory still used back then).

For the SAP system, however, the monitoring office had to check access authorizations manually. Ever since the bank's spin-off, IBB used an SAP system including all key base modules as their central IT system, which also provides the promotional bank's core banking system Abakus with data. Eike Thore Schmaida illustrates the steps involved in manually recertifying access rights. He is in charge of IAM as a member of the IT Governance department of IBB, which was put in place several years ago to keep up with the rising number of regulations: "We had to request the access authorizations from the administrators of the individual systems in tabular format and forward these tables to the managers. They, in turn, compared them against their teams based on questions such as 'who is still in the department, who changed their role and needs access to new systems?' etc. The answers were returned to the administrators, who then made the necessary adjustments in the systems – a process called provisioning."

A Consistent Recertification Solution Was Needed

Yet the managers frequently did not understand the details or implications of individual access rights. This made proper and regular recertification, as is demanded by MaRisk (minimum risk management requirements), difficult to fulfil. Worse yet, the auditing firm insisted on receiving an overview of all access rights updated daily. In order to remedy the overall difficult situation and meet this demand, the bank thus issued an invitation to tender in 2015 to find a suitable IAM system. The bank was also looking into introducing a consistent recertification solution as part of this system change.

Extremely Quick Implementation

Beta Systems was awarded the project, "because they have long-standing expertise in the banking sector," says Percy Frahm, Department Head Technical Infrastructure at Investi-tionsbank Berlin. "The provider had competent answers to all our questions regarding IAM that also convinced the auditors." The recertification portal that comes with the suite (and which requires no programming on the customer's side) as well as the predefined role profiles provided further incentives to choose the Beta Systems solution. Also, it took only a little longer than half a year to implement the solution, which is very quick for this kind of project.

The Recertification Center allows us to perform proper and regular recertification, as required by MaRisk, much more quickly and transparently than was possible using the previous manual process.

———————————

Eike Thore Schmaida
responsible for IAM as a member
of the IT Governance Team at IBB

The new GARANCY Suite allowed IBB to completely redefine their authorization monitoring and assignment processes. The new workflow does not depend on various people across the company replying to a request. Instead, the software autonomously collects required data from the connected systems and automatically prompts managers in freely definable intervals to recertify access rights.

The 'GARANCY Identity Manager' provisioning module enables IBB to centrally administrate and control all user-related authorization information (identities, groups, roles) across all IT systems. Access rights are recertified via the web interface of the GARANCY Recertification Center. Here the rights and roles assigned to employees are checked by the defined person in charge and automatically revoked if the manager decides not to extend an authorization. "We now have an out-of-the-box identity access management solution simply not offered by other software providers," says Eike Thore Schmaida, providing a further reason why the bank chose Beta Systems.

Predefined Standard Workflows from Beta Systems
In half a year's time, 40 systems were connected to the GARANCY Suite. The uConnect technology even allows for integrating individual IT applications via flexible interfaces such as CSV. The HR system delivers the current master data to GARANCY each day in a unidirectional transfer. GARANCY then analyzes the data and captures users. For this process IBB is using a predefined Beta Systems standard workflow to which additional approver steps were added. In essence, it prompts managers to confirm that a given user works in the corresponding department.

When introducing the new IAM system, departments were associated with roles that did not previously exist at IBB. Each department has its own e-mail mailing list, a dedicated directory on the drive as well as access rights for various data processing applications.

"We bundled this information in one role and implemented it in the GARANCY Identity Manager," explains Andre Heilscher, IAM Application Administrator at IBB.

Portal Delivers Excellent Usability and Wealth of Features
The first recertification was performed in the portal in early 2017. It involved 60 managers who had to review the access rights of about 850 users. "The portal's look & feel, its delegation and other quick functions and views greatly simplified the task of recertifying the team members," concludes Percy Frahm. He and his colleagues also found the campaign administrator view and the option of informing users about revoked access rights via mail notification very useful.

On average, each manager checks the access authorizations of 10 to 20 employees to the various systems. Percy Frahm, who is also a staff manager, was in charge of checking roughly 1,400 authorizations. "The Recertification Center illustrates in a highly structured and comprehensible manner the role of any employee and what systems she uses for what purpose. This makes it so much easier to quickly decide on whether to reassign or revoke access to an application." Thanks to this overview, he was able to delete one third of the authorizations right then and there. Once changes are made with GARANCY, the tool automatically revokes the respective role(s). Owing to this speedy workflow, the entire recertification took him only half a working day.

Other managers also made quick progress, so the entire cycle was completed in just six weeks. The information provided by the solution also allows the monitoring office to keep track of which managers are lagging behind and send them reminders. This further accelerates the overall process.

Beta Systems was awarded the project as they have long-standing expertise in the banking sector. The provider had sound answers to all our questions regarding IAM that also convinced the auditors.

Percy Frahm
Percy Frahm, Department Head Technical Infrastructure at Investitionsbank Berlin

Outstanding User Management According to Auditors

Andre Heilscher: "The quality of the assigned authorizations has clearly improved ever since introducing the GARANCY Suite. We were able to identify numerous obsolete roles and potential for extending role bundles. The entire identity management process has been centralized, and we now administrate all access rights for any system in a comprehensive and consistent manner, rather than in the piecemeal fashion employed before."

The auditing firm that recently performed an IT check in preparation for a Section 44 Banking Act check (readiness check) also noticed that things had changed at IBB. This check is based on the 'Bank IT Supervision' regulation part of MaRisk. "A 44 check is probably the toughest check that a bank can be subjected to," knows Eike Thore Schmaida. But in this case there were no complaints. As regards the IBB's authorization management and certification processes, the auditing firm 'strongly recommended' the technology in place.

In the meantime, the bank is further expanding the solution. By upgrading to the latest version at the end of 2017, the bank will be able to use the GARANCY Suite to perform role recertification without the present limitation of certifying individual users. The expansion also involves connecting new target systems and special management tools or even the network switches, which are also protected by means of user authentication.

About the Company

IBB is the promotional bank of the state of Berlin. It actively supports the economic development of Berlin and provides consulting on questions regarding real estate subsidies and financing matters. IBB promotes economic development mainly through loan- and equity-based financing made available via revolving development funds. The corporate history includes overcoming the housing crisis in the 1920s, balancing structural deficits after the German reunification and performing monetary economic development measures in the 21st century.

Facts & Figures

Year of founding: 1924 (originally as Wohnungsfürsorgegesellschaft Berlin mbH)
Employees (2016): 620
Head office: Berlin
Chairman of the Board: Dr. Jürgen Allerkamp
Sector: Financial services

Challenge

Increasing regulations for the finance industry made inspecting, assigning, renewing and revoking access rights for the various IT systems a time-consuming and error-prone affair at IBB. This is why the bank decided to replace the manual process with fully automatic identity access management.

Products Employed

GARANCY Identity Manager, GARANCY Process Center, GARANCY Recertification Center

Benefits of the Beta Systems Solution

Ever since introducing the GARANCY Suite, IBB's new workflow no longer depends on various people across the company replying to a request. Instead, the software autonomously collects required data from the connected systems and automatically prompts managers in freely definable intervals to recertify access rights.

Competitive Advantage

As part of an IT audit performed in preparation for a Section 44 Banking Act check (readiness check), the auditing firm working with IBB found that the bank's authorization management and certification workflows serve as a 'best practice model for the promotional banking sector'. Automated and streamlined IAM processes enable the IT department and management to dedicate more time to customer-facing activities.

Key Figures

Connected systems: 120
Defined roles: approx. 70 OE roles, approx. 3,500 actual roles
Implementation time: ten months
Time required to perform a recertification cycle: six weeks