



Enhanced Security and Compliance with IAM at KGAL GmbH & Co. KG

Leading German Real Asset Management Company
Secures Access to Critical Applications with the Garancy
Identity Manager

A product by  beta systems





About the Company

KGAL is one of Germany's leading real asset managers and manages investments in real estate, sustainable infrastructure, and aviation. Headquartered in Grünwald near Munich, the company serves institutional and private investors and manages approximately 16 billion euros in assets.



● THE CHALLENGE

Replacing Individual Manual Processes

At KGAL, an in-house system supported standard processes related to onboarding and offboarding, but it reached its limits when it came to role management, recertifications, and centralized governance. Manual workflows using Excel and tickets created a significant burden, made traceability difficult, and increased the need for coordination between business units and IT.

● THE SOLUTION

Identity Governance: A New Centralized Approach

Together with Garancy, KGAL implemented the Identity Manager as the central platform for access management. A comprehensive role model comprising basic, organizational, functional, and business roles now forms the basis for assigning permissions. Standard processes were automated, existing systems were integrated, and recertifications were incorporated into a central workflow. At the same time, this enabled the teams in charge to make many adjustments on their own.

● THE RESULT

Greater Security, Transparency, and Efficiency

Today, KGAL manages access rights centrally and in a traceable manner. Automated joiner, mover, and leaver processes reduce the workload on IT, recertifications can be carried out much more easily, and compliance requirements are reliably supported. At the same time, centralized management ensures greater transparency regarding existing access rights and reduces the risk of unauthorized access.

A centralized IAM solution is vital for building a modern and secure IT environment. Any company aiming to professionalize their access management should invest in IAM. With Garancy, we made the right choice.



Ludwig Eggersdorfer
Head of Digital Workplace, IT-Governance
& Infrastructure Solutions

Technology, Processes, and Roles Seamlessly Integrated

Out-of-the-Box Functionality

KGAL had previously relied on an in-house development called the "Employee Hub," which handled HR lifecycle processes such as onboarding, offboarding, and employee transfers as well as their corresponding access rights. However, it lacked robust capabilities for role management and regular recertification. After a careful evaluation of multiple vendors in 2022, KGAL selected the Garancy Identity Manager. The solution has been live since July 2023.

Bernd Stiller, Project Manager Digital Workplace at KGAL, says: "As a mid-sized company, we value working with a collaborative technology partner – with dedicated contact persons who respond quickly to our requests. Of course, the software also must be excellent and match our requirements."

He particularly highlights the software's recertification capabilities and praises its out-of-the-box functions for implementing standard processes, such as employee onboarding, offboarding, and department changes. The solution is also highly flexible and adaptable to individual organizational requirements.

Ludwig Eggersdorfer, Head of Digital Workplace, IT-Governance & Infrastructure Solutions, adds: "As a German provider, Garancy is familiar with the regulatory requirements of the industry, including those of the German Federal Financial Supervisory Authority (BaFin). That is incredibly valuable to us."

System Integration via uConnect

The connector technology from Garancy enables seamless integration of all KGAL systems into the Identity Manager. Many applications use Active Directory (AD) groups for access rights management. Once an access request is approved in Garancy, the corresponding rights are automatically assigned.

For systems that do not support automated provisioning, rights are entered manually. By integrating the ticketing system, Garancy automatically creates and tracks the respective authorization tickets. Available rights are described in clear, user-friendly terms, ensuring no misunderstandings between business users and IT administrators. This eliminates unnecessary rework and avoids media discontinuities.

As a mid-sized company, we value working with a collaborative technology partner – with dedicated contact persons who respond quickly to our requests.



Bernd Stiller
Project Manager Digital Workplace

Role Concept as the Foundation of Access Management

A well-designed role concept is always key to successful IAM implementation. While an initial role framework existed before the project, it was only through the introduction of Garancy's IAM solution that the structure was fully developed at KGAL. Today, it consists of four role types:

- **Base Roles** – Automatically assigned to all internal and external employees and include basic permissions required by everyone.
- **Organizational Roles** – Assigned according to the employee's organizational unit, covering the rights necessary for their departmental tasks.
- **Functional Roles** – Based on an individual's function and include additional, role-specific permissions.
- **Specialized Roles** – Granted for specific duties or responsibilities, such as external service providers like auditors or tax consultants.

The Recertification Center allows us to monitor the progress of updates much more effectively, access systems through individual employees, and check their authorizations.



Sabine Mehner
Vendor Management

Sabine Mehner from Vendor Management oversees the access rights of external service providers and can manage them with fine granularity thanks to the specialized role model. She is particularly enthusiastic about the simplified recertification process.

Before the IAM introduction, this was a time-consuming and error-prone process, managed via Excel and ticket systems. For each application, she received a separate list, showing who had access. She had to go through them line by line, often clarifying details individually. "It sometimes took one or two weeks," she recalls.

Thanks to the Recertification Center, Sabine Mehner can now easily monitor the progress of updates, check each employee's access rights across all applications, and review permissions directly within the system. "It's still work, but it's significantly less effort than before", she says.

A Partnership-Based Approach

KGAL describes its collaboration with Garancy as consistently positive. "We made it our goal from the beginning to build in-depth internal know-how, so we don't have to outsource every change to the Garancy team. They have supported us excellently in this approach and are always there with advice and assistance when needed," explains Bernd Stiller.

For larger projects or change requests, the two companies work closely together to develop tailored solutions – a collaborative partnership based on open communication.

Conclusion: IAM as an Essential Element for Secure IT Operations

The implementation of the Garancy Identity Manager has proven to be a highly worthwhile investment for KGAL. By centralizing their access management, the company has significantly enhanced its IT security and reduced the risk of unauthorized access.

The implemented IAM solution ensures compliance, particularly through automated recertification, and improves efficiency by automating standard employee lifecycle processes. In addition, transparency has increased: Centralized management provides a comprehensive overview of access rights and simplifies compliance monitoring.

"A centralized IAM solution is vital for building a modern and secure IT environment. Any company aiming to professionalize their access management should invest in IAM. With Garancy, we made the right choice," concludes Eggersdorfer.

Facts & Figures

● FOUNDED

1968

● EMPLOYEES

approx. 400

● HEADQUARTERS

Grünwald, Germany

● INDUSTRY

Financial Services/
Asset Management

KGAL has been investing in real assets for decades and combines long-term investment strategies with high regulatory requirements.

Success Thanks to Garancy

- Automated joiner, mover, and leaver processes
- Flexible role models for internal employees and external service providers
- Significantly simplified recertification of permissions
- Reduced manual workload for IT and business units
- Greater transparency, compliance, and traceability
- Independent administration of numerous customizations without vendor support

Products Used at KGAL

- Garancy Identity Manager
- Garancy User Center
- Garancy Recertification Center
- ConPack
- uConnect Advanced

Ready to Unlock New Opportunities?

Get in touch to explore how Garancy can support your IAM strategy.

✉ hello@garancy.com

☎ +49 (0) 30 726 118-0