beta systems

KGAL
REAL INVESTMENTS

Enhanced Security and Compliance with IAM at KGAL GmbH

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

Headquartered in Grünwald near Munich, KGAL GmbH has laid the foundation for modern, secure, and efficient access management by introducing a comprehensive Identity Management solution. The established German investment and asset management company operates both on-premises and cloud-based applications.

> ” *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 Beta Systems, we made the right choice.*
>
> **Ludwig Eggersdorfer**
> Head of Digital Workplace, IT-Governance & Infrastructure Solutions

About the Company

Based in Grünwald near Munich, KGAL GmbH & Co. KG has been a leading German real asset manager for more than 40 years, specializing in long-term real capital investments with stable, sustainable returns.

Its portfolio includes the design and management of public and institutional investment funds, as well as tailored solutions for family offices and foundations.

KGAL offers investors opportunities in Real Estate, Sustainable Infrastructure, and Aviation, and invests in innovation through Venture Capital & Private Equity. In 2025, the company's investment volume totaled approx. €16 billion.

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 from Beta Systems. 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 technology partner at eye level – 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.

> *As a mid-sized company, we value working with a technology partner at eye level – with dedicated contact persons who respond quickly to our requests.*
>
> **Bernd Stiller**
> Project Manager Digital Workplace

Ludwig Eggersdorfer, Head of Digital Workplace, IT-Governance & Infrastructure Solutions, adds: "As a German provider, Beta Systems 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 Beta Systems 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.

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 Beta Systems' 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 oneor 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 Beta Systems 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 Beta Systems. 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 Beta Systems, we made the right choice,” concludes Eggersdorfer.

KGAL
REAL INVESTMENTS

Facts & Figures

Founded: 1968
Employees: approx. 400
Headquarters: Grünwald, Germany
Co-Managing Directors:
Florian Martin, André Zücker

Industry

Financial Services

The Challenge

Manual management of IT access rights was time-consuming and error-prone, leading to potential compliance issues and inefficiencies. KGAL GmbH sought to automate this process through a comprehensive Identity and Access Management solution.

Benefits of the Solution

The company now uses a role-based model with basic, organizational, functional, and specialized roles to automatically assign and revoke access rights. The IAM system has streamlined and accelerated the process of recertification, significantly reducing effort for both IT and business departments. Most adjustments can now be made internally without the need to consult Beta Systems.

Competitive Advantage

The Garancy Identity Manager automates the provisioning and removal of access rights during employee onboarding, offboarding, and role changes. This greatly reduces manual workload for IT and management, freeing resources for customer-focused tasks.

Key Metrics

- Connected Systems: 30
- Organizational Roles: 80
- Specialized Roles: 30
- Users (internal and external): 800

Products Used

- Garancy Identity Manager
- Garancy Order Portal
- Garancy Recertification Center
- ConPack
- uConnect Advanced