



beta systems



Garancy® Suite

Strengthen Your Organization's Cyber Hygiene with Identity Access Management

Garancy – Your First Line of Defense

The need to properly manage user identities and limit related access rights to the minimum required for a given role in the organization is continually increasing. Therefore, Identity Access Management (IAM) should be on the agenda of every IT Security Manager.

With Garancy, the IAM software solution from Beta Systems, companies ensure that all access rights to data and applications are controlled and monitored. This is done according to organizational requirements and user roles by associating user rights and restrictions with the established identity.

” *Insider threats cause 200% more damage than external attacks.*

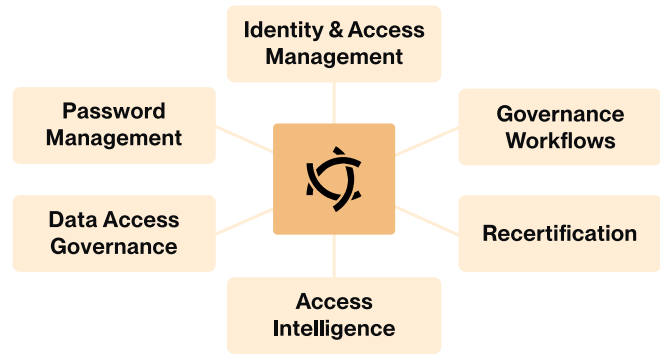
Source: Carnegie Mellon University

Fact Check

- The number of attacks on information security is growing.
- Worldwide, more than 42.8 million incidents are registered per year – that's nine attacks per second.
- 60% of the attacks originate from insiders.
- The damage caused by insider attacks is 200% higher compared damage caused by external attacks.
- Many companies still underestimate internal security risks.

Modules of the Garancy Suite

The Garancy modules cover all tasks of Identity Access Governance and are available for on-premise and cloud deployments.



IAM – Bridging Business and Security

The Provisioning module is a central point for administering and controlling all access credentials for users (identities, groups, roles) across all IT systems.

Provisioning

- Integration of IT applications through a wide range of out-of-the-box connectors
- Flexible and scalable synchronization between identity management and target systems
- Provisioning, consolidation and synchronization of access rights
- Real-time implementation of changes

Access Governance

- Role Lifecycle Management with role hierarchies
- Automatic role assignment based on identified user profiles
- Enforcement of SoD rules (Segregation of Duties)
- Manage authorizations based on roles and internal IT security policies

User Management

- Automated HR data import
- Management of the entire user lifecycle (Joiner, Mover, Leaver)
- Differentiation between different user types, e.g. internal and external employees

Audit and Security

- Set audit trails for allocated rights
- Single point of information and enforcement of access policies
- Independent administration of multiple objects through a central IAM platform

Involving Business Departments through Governance Workflows

With governance workflows in Garancy, customers can digitize their processes and accelerate all activities related to access rights. Business departments are directly involved while ensuring compliance with IT security policies. Assigned permissions remain fully traceable and auditable.

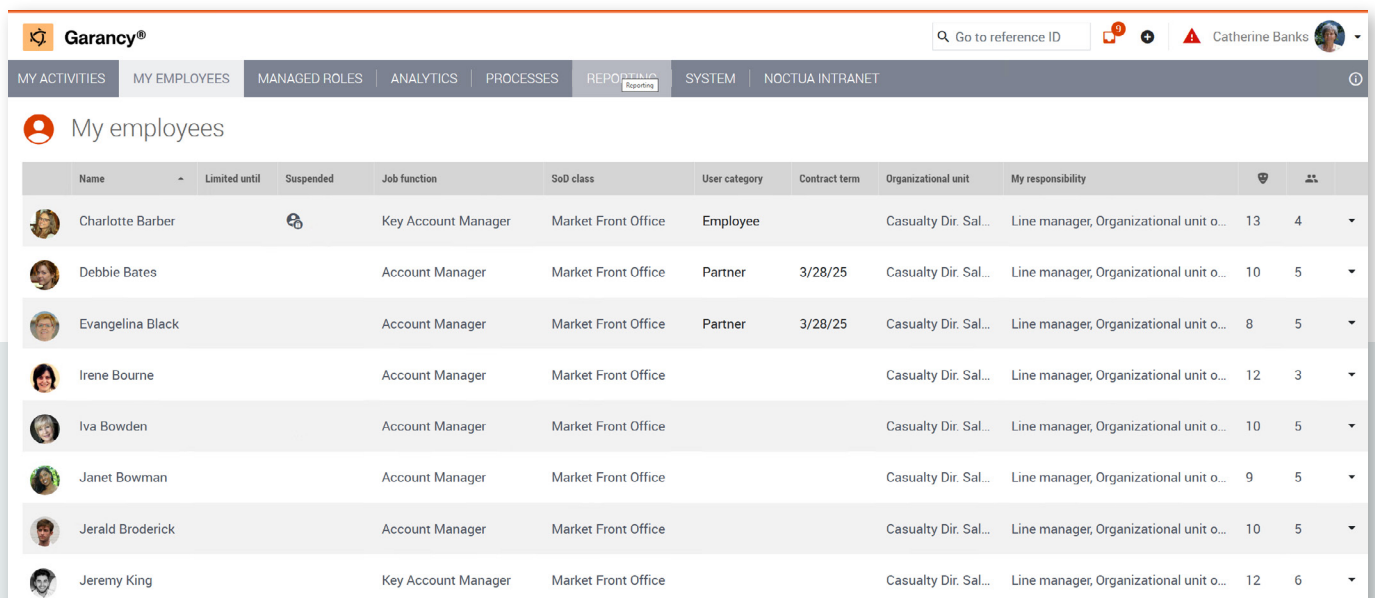
The responsibility for managing access rights lies with the respective business units.

- Shorter processing times for access approvals
- Complete traceability of access rights assignments
- Increased user satisfaction thanks to immediate access to needed resources
- Compliance with regulatory requirements and industry standards
- Reduced workload for IT administrators through business department involvement
- Faster turnaround times for all approval workflows

Recertification of Access Rights

With the web-based portal for efficient access rights recertification, permissions for internal and external users can be centrally assigned, reviewed, or revoked. This increases security and improves the accuracy of assigned authorizations.

- Recertification campaigns based on organizational structures, role profiles and risk assessments
- Substitution and delegation via integrated workflows
- Multiple view options, e.g. single-user view, group overviews and SoD violations
- View recertification status in real-time – including due dates, revoked and confirmed permissions
- Quick recertification and automatic out-of-the-box deprovisioning
- Auditable campaigns with complete event logging and archiving
- Optimized for desktop use and mobile work via tablets or smartphones



Name	Limited until	Suspended	Job function	SoD class	User category	Contract term	Organizational unit	My responsibility		
Charlotte Barber			Key Account Manager	Market Front Office	Employee		Casualty Dir. Sal...	Line manager, Organizational unit o...	13	4
Debbie Bates			Account Manager	Market Front Office	Partner	3/28/25	Casualty Dir. Sal...	Line manager, Organizational unit o...	10	5
Evangelina Black			Account Manager	Market Front Office	Partner	3/28/25	Casualty Dir. Sal...	Line manager, Organizational unit o...	8	5
Irene Bourne			Account Manager	Market Front Office			Casualty Dir. Sal...	Line manager, Organizational unit o...	12	3
Iva Bowden			Account Manager	Market Front Office			Casualty Dir. Sal...	Line manager, Organizational unit o...	10	5
Janet Bowman			Account Manager	Market Front Office			Casualty Dir. Sal...	Line manager, Organizational unit o...	9	5
Jerald Broderick			Account Manager	Market Front Office			Casualty Dir. Sal...	Line manager, Organizational unit o...	10	5
Jeremy King			Key Account Manager	Market Front Office			Casualty Dir. Sal...	Line manager, Organizational unit o...	12	6

Figure 1 – Overview of employees

Secure Password Management

Password management enables secure and seamless access for computers to various IT platforms or applications across distributed systems. It helps enforce IT security policies related to password usage more effectively.

Password Reset allows users to reset and change their passwords independently through a web-based interface. This significantly reduces helpdesk workload and increases user productivity by minimizing downtime.

Password Synchronisation enables employees to access multiple platforms and applications using a single password. Any password changes are automatically synchronized across all connected systems and are instantly available to the user across environments.

Reporting and Analytics with Access Intelligence

The Access Intelligence module leverages Business Intelligence to manage access rights effectively. The solution provides reports and multidimensional analyses to audit permission structures within the organization and identify potential access risks.

- 360 monitoring: Full visibility into access rights and associated risks
- Intuitive dashboards offer a comprehensive overview of key security indicators
- Business-oriented, user-friendly reporting and audit tools for out-of-the-box analyses or custom reports
- Dynamic historization: All changes are immediately detected and fully traceable
- Fast correction of authorization errors or security vulnerabilities
- Data-driven access control and improved governance based on actionable insights

Managing Unstructured Data with Data Access Governance

The volume of unstructured data – such as spreadsheets, documents, presentations, or emails – is growing rapidly. In addition to traditional IAM solutions, a structured access rights management approach is becoming essential.

Data Access Governance provides a specialized module for managing and controlling access rights to unstructured data. Fully integrated into Garancy, it reduces helpdesk workloads and enhances overall transparency.

- Data owners manage access independently – without direct IT involvement
- Integrated compliance checks involving business departments
- Automated enforcement of internal policies and legal requirements
- Policy-compliant access rights assignment through business-driven request and approval workflows
- Real-time detection of critical deviations via entitlement reconciliation
- Garancy as a single point of administration – also available as a portal-based stand-alone solution

Ready to Take the Next Step?

Contact us to learn more about our IAM solution – we look forward to hearing from you.

Email us at info-iam@betasystems.com or give us a call at **+49 (0) 30 726 118-0**.



www.betasystems.com/products/garancy