_betasystems

GARANCY IAM SUITE

The best-fit Identity & Access Management solution for dynamic companies!

60% of all data thefts are caused by insiders…

… and caused 200% more damage than from the outside!

Beta Systems IAM is your first line of defense

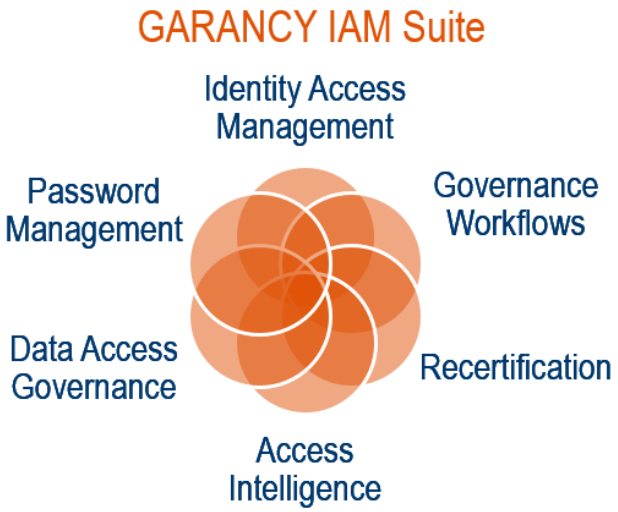
Fact Check:

- Growing number of attacks on information security
- Worldwide registration of >42,800,000 incidents p.a. / 9 attacks per second
- 50-70% of attacks are caused by insiders
- Insider attacks are causing 200% of the damage compared to attacks from the outside
- Still companies underestimate the risk from within the organization

The need to properly manage user identities and limit the related access rights to the minimum required for a given role in the organization is continuingly increasing. Therefore Identity Access Management (IAM) should be on the 2019 agenda of IT security managers.

With Beta Systems Identity Access Management Suite companies can ensure all access rights to data and applications are controlled and monitored. This is done according to organizational requirements and users' roles by associating user rights and restrictions with the established identity.

The modules of the GARANCY IAM Suite
The modules of Beta Systems' IAM suite cover all required components of Identity Access Governance. They are available in the cloud as well as on premise.



Identity Access Management – Bridging Business and Security

Our Provisioning module allows for collection and administration in a central repository for all information associated with users (identities, groups, roles), with components of your IT system (target systems) and with access rights:

Provisioning

- Connect and control systems through one of the largest choices of out-of-the-box connectors on the market.
- Flexible and scalable reconciliation between Identity Access Management and targeted systems.
- Collection, normalization and reconciliation of access rights.
- Real-time propagation of modifications.

User Management

- Automate imports of HR data
- Automate the user-lifecycle (joiners, leavers, and movers).
- Distinction between different user types (e.g. internal and external employees)

Access Governance

- Role Lifecycle Management with flexible role hierarchies.
- Role mine and automate assignment of roles depending on identified profile for a given user.
- Enforce prevention and corrective SOD rules (segregation of duties).
- Manage authorizations based on roles and internal IT security policies.

Audit and Security

- Set audit trails for allocated rights.
- Historization and access rights and modifications.
- Single point of information and application of access policies.
- Independent management of several entities over a single IAM platform.

According to AT Kearney 30,000,000 attacks on information security came from within the companies in 2014!

Insider attacks are causing almost 200% more damage
per case compared to attacks from the outside on average!
Study of Carnegie Mellon University

Governance Workflow – Involving the Business Layer

The use of Governance Workflows in your IAM system allows you to digitally design and accelerate all your processes associated to access rights.

Involve business departments while simultaneously guaranteeing the enforcement of your IT security policies and the traceability of assigned access rights.

Delegate the management of access rights entitlement to the business departments.

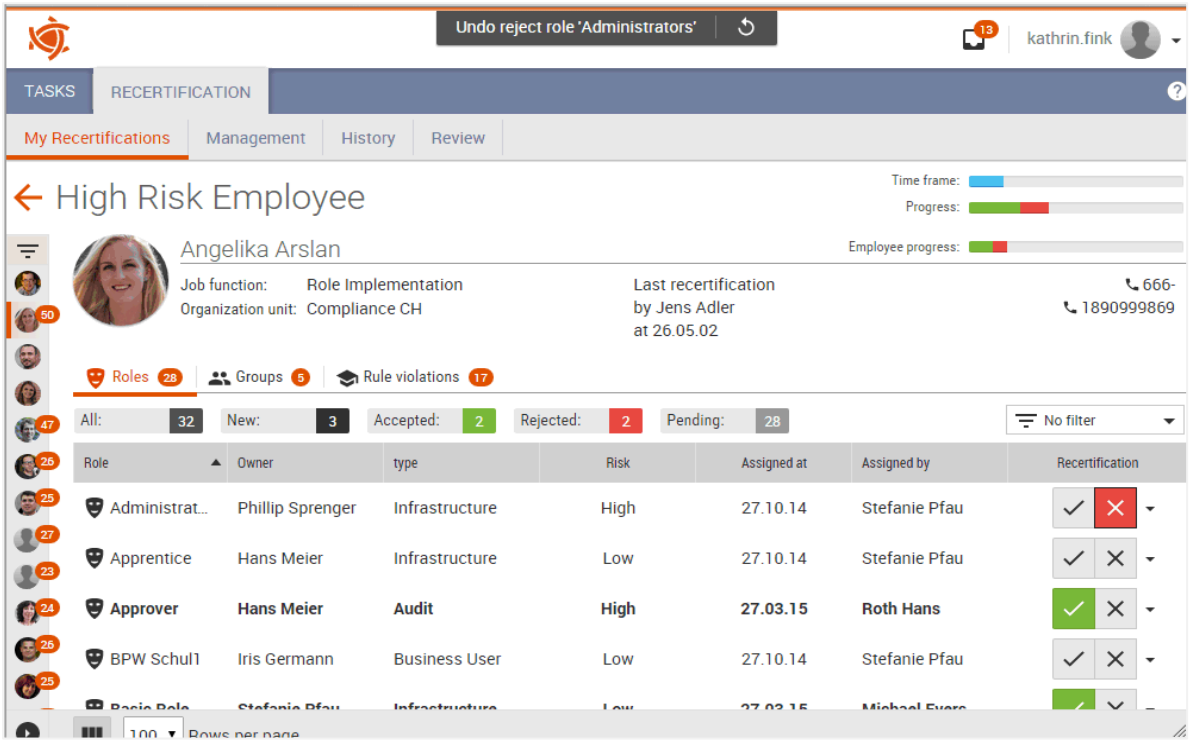
- Shorten process time associated to requests.
- End-to-end traceability: from the assignment of access rights to their implementation into the target systems, and back to the origin.
- Improve end user satisfaction: they rapidly get the appropriate access.
- Ensure compliance to your process regarding legal requirements, norms and standards.
- Reduce workload of IT administrators thanks to a higher implication of business departments.
- Shorten throughput times of all your workflows.

Recertification of Access Rights – Never trust: Always verify

Our browser-based solution for the efficient recertification of access rights enables companies to review internal and external users' access rights and to specify which managers are able to recertify or revoke user permissions.

The company benefits from an increase in the security and efficiency of recertifications, while making the recertification process itself auditable and compliant.

- Risk-level driven recertification and revocation of access rights.
- Recertification campaigns based on org units, job titles or risk assessments.
- Scheduled or ad-hoc recertification campaigns.
- Substitution / delegation via workflows.
- Lots of views: single user view, group overview, list of SoD violations, cross-table comparisons...
- Recertification progress bar with details on expiry date, description, revoked and recertified entitlements as well as time frame.
- Automatic de-provisioning (immediately or scheduled) after completion of recertification.
- Auditable campaigns: complete event logging and archiving of the progress status.
- Optimized for usage on desktop, tablet or mobile devices



Password Management – Secure and efficient

The Password Management module facilitates access to applications and simplifies the enforcement of IT security policies associated to passwords.

Password Reset allows users to reset or modify their own passwords using a web interface.

- Reduce Helpdesk interventions by delegating password reset to users.
- Increase users' productivity as they can reset passwords without waiting on Helpdesk.

Password Synchronization enables the use of a single password to access systems and applications. It ensures changing a password on one system results in the automatic update of the password for all related accounts on all other systems.

Access Intelligence – Reporting & Analytics

The Access Intelligence module utilizes business intelligence to manage access rights. The solution provides reports and multidimensional analysis that help audit the authorization structure of the company, and thus identifies potential risks.

- 360° dynamic monitoring: mapping of access rights and associated risks.
- Full picture of security indicators, in form of ergonomic dashboards.
- Business oriented and easy to use reporting and auditing tools: out-of-the-box or customized reports.
- Dynamic historization: every change made is identified, tracked, and instantly available for consultation.
- Quick correction of authorization errors or security breaks. Secure access structure and improved governance based on proven facts.

Data Access Governance – Management of unstructured data

Unstructured data and information are loosely scattered in file systems, document systems, Sharepoint or email systems. They are demanding a well-structured access rights management in addition to a conventional Identity Access Management solution.

The Data Access Governance (DAG) module offers a specialized administration and control module for the access and control of such unstructured data and is fully integrated in the Beta Systems' IAM suite.

- Business departments control the access without direct intervention by IT.
- Integrated compliance checks with the integration of the data owner in the business departments.
- Automatic compliancy with corporate and regulatory policies to control access to critical data.
- Access rights management with approval workflows and roles: no more rights awarding bypassing the control processes.
- Immediate uncovering risky deviations of the actual from the target state.
- Beta Systems' IAM as single point of contact. Also available as portal based stand-alone solution.

betasystems

Beta Systems IAM Software AG

Alt-Moabit 90d | 10559 Berlin | Germany
Phone: +49 (0) 30 726 118-0 | Fax: +49 (0) 30 726 118-800
iam@betasystems.com | www.betasystems-iam.com

Beta Systems Partner: