Use Access Intelligence to minimize Access Risks!

ACCESS INTELLIGENCE & ACCESS RISK MANAGEMENT

Our analyses and reports deliver the whole spectrum of security-relevant information, such as number of roles, groups, accounts or target systems per user including historical analyses of access rights. Dedicated dashboards providing weighted data and key risk indicators allow staff to perform targeted follow-up measures.

Risk-based access intelligence methods can uncover critical security gaps and thus help prevent any form of data misuse. Our solution offers automatic support throughout all stages of access risk management – from assessment and analysis through to monitoring and risk control.
Companies are increasingly faced with the challenge of handling vast amounts of data generated by complex IT systems, as well as implementing and enforcing access control measures based on identity & access governance. At the same time, compliance requirements need to be adhered to, both in terms of providing data transparency and averting dangers and risks by putting optimized access management workflows into place.

Garancy Access Intelligence Manager is a powerful analysis tool for

- monitoring a broad range of data sources
- historical analyses of access rights with the GARANCY TIME TRAVELER add on.
- meeting compliance provisions
- preventing identity abuse or threats from insiders.

Garancy Access Intelligence Manager offers reliable answers to new IT challenges posed by legal compliance regulations. The solution brings transparency and security to business processes and allows them to be reviewed retroactively. The product does this by analyzing all business-relevant data sources and providing information in the shape of individualized drill-down and drill-through reports.

**ACCESS INTELLIGENCE**

Access Intelligence provides huge analytical capabilities that will procure in-depth insight into access right structures. It is this insight that will enable the right decisions to be taken as the basis for enterprise wide access governance activities.

Therefore this opens up completely new possibilities for Governance activities that can be used immediately for the analysis and preparation of data from user provisioning systems.

Access authorizations are increasingly managed by the corporate specialist departments. This is why Garancy Access Intelligence Manager provides the people in charge with all relevant user data in a comprehensible manner and offers three analysis methods at the push of a button:

**ACCESS RISK MANAGEMENT**

Our risk-based access intelligence methods go beyond merely managing the allocation of access authorizations. They can uncover critical security gaps and thus help prevent any form of data misuse.

Garancy Access Intelligence Manager provides automated support during all risk management stages.
Audit Analyses focusing on “internal and external audit” while taking GRC aspects into consideration.

The importance of an effective internal control system (ICS) in preventing and detecting obvious compliance gaps is clear. The link between the compliance management system and the ICS centers on the following questions:

- Does the existing ICS have sufficient and appropriate controls to cover the identified and assessed compliance risks (control design)?
- Do existing controls prevent or detect enterprise-wide compliance effectively (control effectiveness)?
- Who had access rights to data and applications at any given point in the past?

Business Analyses focusing on “business-relevant issues” including user access authorizations

As access authorization management is increasingly shifting from IT to specialist departments, this makes it necessary to provide the relevant user data in a format readily understood by non-technicians. Management dashboards, business analyses and deviation analyses provide the manager in charge with easy-to-interpret information (e.g. number of roles, groups, accounts, target systems), ensuring that the manager is fully informed about all security-relevant authorizations allocated in the department. In addition to standard reports, there is also the option of launching ad-hoc analyses via drag & drop in order to get solid answers to specific questions.

Administration Analyses focusing on “technical relationships” relevant to IT administrators

Administration analyses create a link between the technical perspective and the business perspective. It compiles and organizes permission data by individual user and features an intuitive user interface developed especially for non-techies. This solution lets the departments not only create powerful analyses but also use them appropriately, thus alleviating the IT administration workload.

Weaknesses in the organization can be directly identified and recommendations for reducing access risk formulated.
APPLICATION FEATURES

REPORTING & AUDITING
- Critical and reliable tools that provide data for audits and help you meet compliance requirements.
- Standard reports according to traditional audit questions and also offer a drag-&-drop mechanism for selecting items based on customer-specific criteria.
- Detailed compliance reports on business processes or deviation reports.

ACCESS RISK MANAGEMENT
- Risk assessment in terms of risk type and risk rates.
- Determine the risk scores of individual users.
- Categorized risk determination (not just a list of risk items).
- Risk assessment with a focus on roles, groups, resources or authorizations.

BUSINESS ANALYTICS
- Provide the relevant user data in a format readily understood by non-technicians.
- Role overviews; Users and their authorizations; Role-group relationships; User counter, and more.
- Ad-hoc analyses options for specific queries.

HIGH RISK USER
- Identify and analyze high-risk users.
- Establish the total risk of a user according to risk class.
- Provide an overview of the risk composition.
- Point out the origin of the risk.
- Provide a basis for taking risk reduction measures.

DASHBOARDS
- Dashboards offering weighted information and key risk indicators.
- As indicators can be freely selected, the dashboards provide a complete overview of the corporate authorization structures.
- Highly flexible: Even spur-of-the-moment questions on access management can be answered in a flexible, fast and customizable manner.

BUSINESS DEPARTMENT
- Easy-to-interpret information, ensuring that the manager is fully informed about all security-relevant authorizations allocated in the department.
- Ready-for use reports and analysis options.
- Delivery of push information on a regular basis.

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

Berlin | Cologne | Neustadt | Calgary | Washington D.C. | Vienna
Paris | Madrid | London | Stockholm | Milan | Brussels