



GARANCY ACCESS INTELLIGENCE MANAGER

Risikominimierung durch bedarfsgerechte Informationen!

ACCESS INTELLIGENCE & ACCESS RISK MANAGEMENT

Unsere Analysen und Reports liefern sämtliche sicherheitsrelevante Berechtigungsinformationen, wie z.B. die Anzahl an Rollen, Gruppen, Accounts oder Zielsystemen pro Benutzer einschließlich historischer Analysen. Entsprechende Dashboards mit gewichteten Aussagen und Key Risk Indikatoren ermöglichen zielgerichtete präventive und Follow-Up-Aktivitäten.

Die Lösungen rund um die Vergabe und Verwaltung von Zugriffsrechten unterstützen alle Phasen des Risikomanagement – von der Risiko-Bewertung und dem Risiko-Monitoring bis hin zur präventiven Risiko-Steuerung.



VERTIEFEN SIE SICH IN DETAILS, UM DAS WESENTLICHE ABZULEITEN

Unternehmen stehen immer mehr vor der Herausforderung, die von komplexen IT-Systemen generierte Datenflut und die damit verbundene Zugriffskontrolle durch Identity & Access Governance zu bewältigen. Auch die Compliance-Anforderungen zielen neben der Datentransparenz konkret auf das **Abwenden von Gefahren und Risiken durch Optimierung des Zugriffsmanagements**.

Der Garancy Access Intelligence Manager ist das wirksame Analysetool für

- die Überwachung unterschiedlichster Datenquellen
- **Historische Analyse der Zugriffsberechtigungen** durch das **GARANCY TIME TRAVELER Add on**
- die Erfüllung von Compliance-Anforderungen an die Zugriffsberechtigungen
- die Vermeidung von Identitätsmissbrauch oder Bedrohung durch Insider.

Die Lösung macht Geschäftsabläufe transparent, sicher und auch rückwirkend bewertbar. Sie analysiert sämtliche unternehmensrelevanten Datenquellen und stellt diese in Form von **individualisierten Drill-down- und Drill-through-Berichten** zur Verfügung.

ACCESS INTELLIGENCE

Access Intelligence eröffnet den Zugang zu leistungsstarken Analysefunktionen, mit denen Unternehmen tiefen Einblick in ihre Berechtigungslandschaft und deren zugrundeliegenden Organisationsstrukturen erhalten.

Diese Informationen bilden das **Fundament für effektive Governance Maßnahmen** im gesamten Unternehmen, die sich unmittelbar zur Analyse und Aufbereitung der in den User Provisioning Systemen generierten Daten nutzen lassen.

Die Zugriffsberechtigungen werden zunehmend von den Fachabteilungen im Unternehmen verwaltet. Deshalb stellt der Garancy Access Intelligence Manager alle relevanten Benutzerdaten in verständlichen Dashboards zur Verfügung und bietet Analysemöglichkeiten mit nur einem Knopfdruck:

ACCESS RISK MANAGEMENT

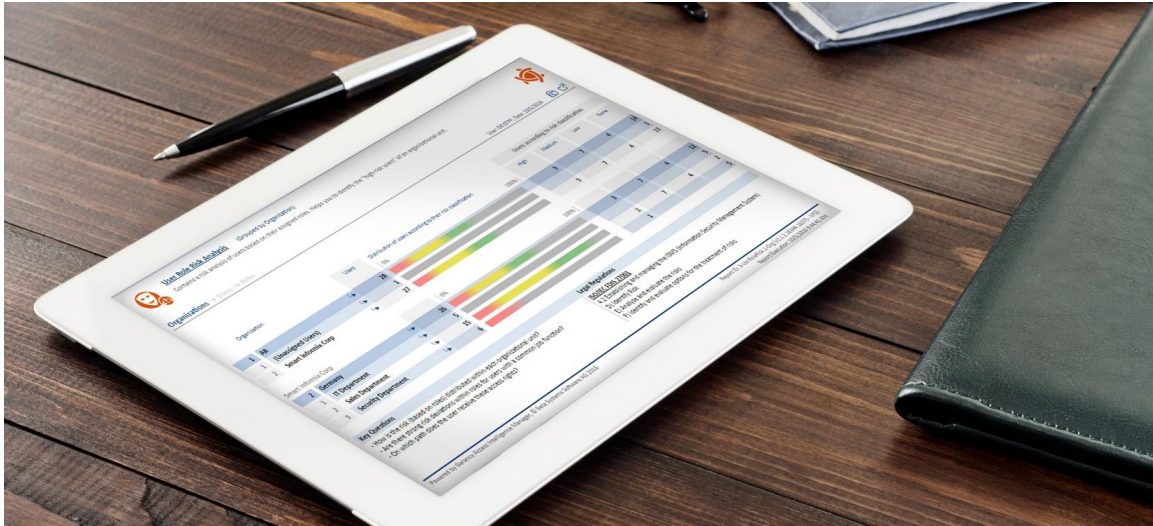
Unsere risikobasierten Access Intelligence Methoden managen nicht nur die Vergabe von Zugriffsberechtigungen. Vielmehr können sie entscheidende Sicherheitslücken aufdecken und jede Form von Missbrauch vorbeugen.

Der Garancy Access Intelligence Manager bietet automatisierte Unterstützung **für alle Phasen des Risiko-Managements**.



Einhaltung gesetzlicher Regularien und Schutz vor Compliance-Verletzungen.

Access Management | Provisioning | Password Management | User Self Service | Governance | Role Lifecycle | Workflow | Recertification | SoD | Compliance Audit | Access Intelligence | Access Risk Management



UMFASSENDE ANALYSE MÖGLICHKEITEN

Audit-Analysen mit Schwerpunkt „Interne und externe Revision“

Hierbei ist die hohe Relevanz eines wirksamen internen Kontrollsystems (IKS) zur Prävention und Aufdeckung von Compliance-Fällen offensichtlich. Die Verknüpfung zwischen Compliance-Management-System und IKS konzentriert sich auf die folgenden Fragestellungen:

- Verfügt das bestehende IKS über ausreichende und angemessene Kontrollen, um die festgestellten und bewerteten Compliance-Risiken abzudecken (**Control Design**)?
- Ist sichergestellt, dass die bestehenden Kontrollen zur Vermeidung oder Aufdeckung von Compliance-Verstößen im gesamten Unternehmen wirksam durchgeführt werden (**Control Effectiveness**)?
- **Wer hatte wann in der Vergangenheit worauf Zugriffsberechtigungen?**

Business-Analysen mit Schwerpunkt „Businessrelevante Fragestellungen“ inklusive Zugriffsberechtigungen von Usern

Da die Verantwortung für Zugriffsberechtigungen immer mehr vom Bereich IT in die Fachabteilungen übergeht, müssen relevante Benutzerdaten in verständlicher Form bereitgestellt werden.

Management Dashboards, Business Analysen und Abweichungsanalysen liefern dem verantwortlichen Manager einfach interpretierbare Informationen (z.B. Anzahl an Rollen, Gruppen, Konten, Zielsystemen), damit dieser alle sicherheitsrelevanten Berechtigungen seiner Mitarbeiter überblicken kann. Neben Standard-Berichten können über Drag & Drop auch Ad-hoc-Analysen zur Erstellung fundierter Antworten auf spezifische Kriterien durchgeführt werden.

Administrations-Analysen mit Schwerpunkt „Technische Beziehungen“ aus Sicht der IT-Administratoren

Administrationsanalysen verknüpfen Berechtigungsdaten mit dem organisatorischen Blick auf jeden einzelnen Benutzer, und dies kombiniert mit einer intuitiven Benutzeroberfläche, die konsequent für Nicht-Techniker entwickelt wurde. Dadurch lassen sich mit unserer Lösung leistungsfähige Analysen durch die Fachabteilungen nicht nur erstellen, sondern auch entsprechend nutzen. Dies führt zu einer Entlastung der IT-Administration.

Schwachstellen in der Organisation lassen sich unmittelbar aufzeigen und Handlungsempfehlungen zur Reduktion des Zugriffsrisikos formulieren.



Sicherheitslücken aufdecken und
Missbrauch vorbeugen.

Access Management | Provisioning | Password Management | User Self Service | Governance | Role Lifecycle |
Workflow | Recertification | SoD | Compliance Audit | Access Intelligence | Access Risk Management

APPLICATION FEATURES

REPORTING & AUDITING

- Datenlieferanten für Audit-Prüfungen und die Erfüllung von Compliance-Anforderungen.
- Standardberichte entsprechend der klassischen Audit-Fragen, per Drag & Drop, Selektion nach kundenspezifischen Kriterien
- detaillierte Compliance-Berichte zu den Geschäftsprozessen oder Abweichungsberichte

ACCESS RISK MANAGEMENT

- Risikobewertung zu Risikotyp und Risikoraten
- Ermittlung des Risk Scores für einzelne User
- klassifizierte Risikoermittlung (keine bloße Benennung von Risikopunkten)
- Risikobewertung auf Rollen-, Gruppen-, Ressourcen und Authorisierungsebene

BUSINESS ANALYTICS

- Relevante Benutzerdaten in verständlicher Form für Fachabteilungen darstellen
- Business Analysen und einfach interpretierbare Informationen (z.B. Anzahl an Rollen, Gruppen, Konten, Zielsystemen),
- Fundierte Antworten erstellen auf spezifische Ad-Hoc Fragen

HIGH RISK USER

- Identifikation stark risikobehafteter Zugriffsrechte
- Aufzeigen der Zusammensetzung und der Herkunft des Risikos
- Grundlage für Sofort-Maßnahmen zur Risikoreduktion
- Ideal auch für die Analyse umfangreicher Datenbanken

DASHBOARDS

- individuelle, kundenspezifische Zusammenstellung von Leistungsindikatoren (KPIs)/ Charts
- Datenstrukturen, Datenmengen, Vorgänge und Risiken
- Benutzer-, Rollen- und Gruppenanzahl
- Flexibilität bzgl. Indikatoren ermöglicht Überblick zu Berechtigungsstrukturen

FACHABTEILUNG

- Einfach interpretierbare Informationen für den sicherheitsrelevanten Überblick hinsichtlich der Zugriffsrechte der Mitarbeiter
- Nutzung vorgefertigter Reports und Analyseoptionen
- Versand regelmäßiger Push Benachrichtigungen und Bildung von Prioritätenlisten

Beta Systems IAM Software AG

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

Berlin | Köln | Neustadt | Calgary | Washington D.C. | Wien
Paris | Madrid | London | Stockholm | Mailand | Brüssel

Beta Systems Partner: