



Identity & Access Management – Mehr als nur IT für das Risikomanagement

Niels von der Hude
Director Product Strategy



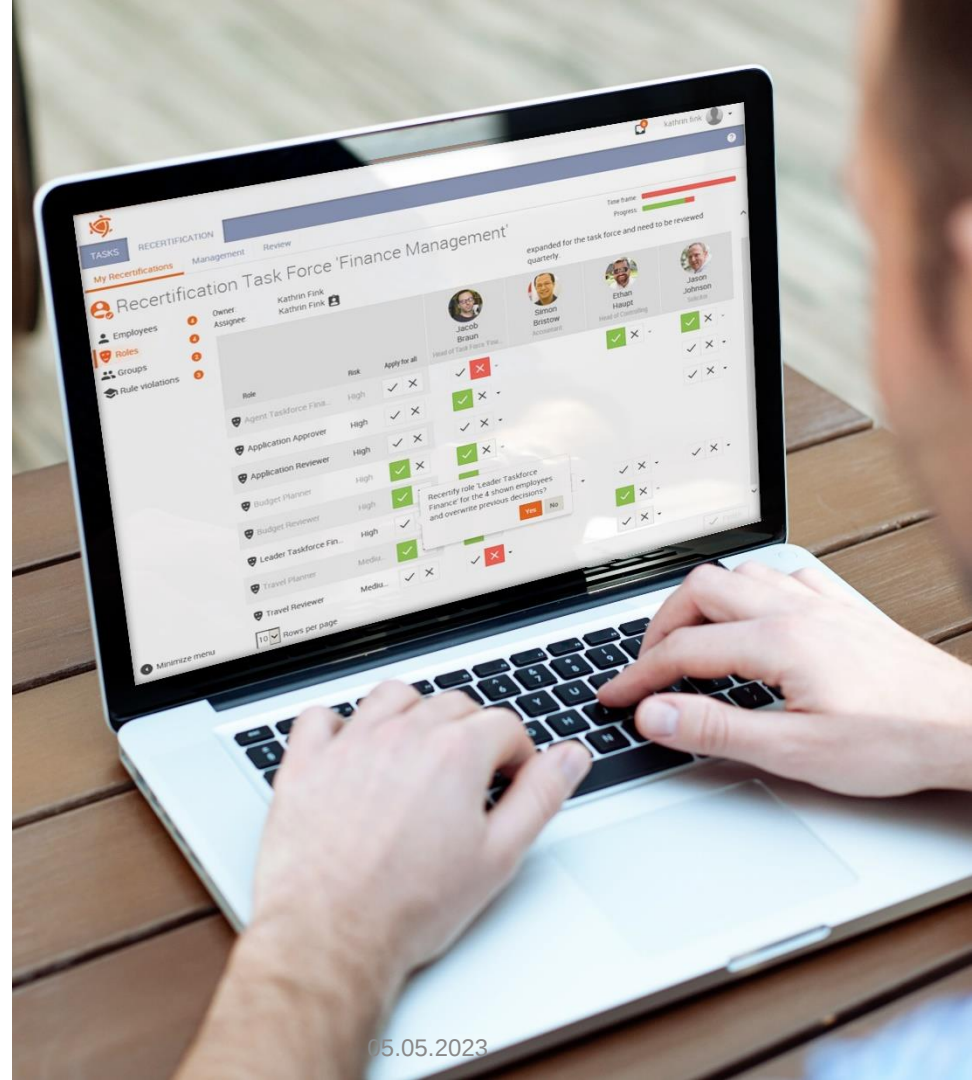
Garancy®

_betasystems



Identity & Access Management

- › **25+ Jahre Identity Management**
- › **Identity Provisioning** für alle Systeme On-Premises und in der Cloud
- › **Access Governance** für Life-Cycle Prozesse, Rezertifizierung & Analysen.
- › **Führender deutscher IAM-Anbieter**



Ein Abstimmung zum Einstieg

Bitte folgen Sie über Ihr Smartphone dem folgenden Link:

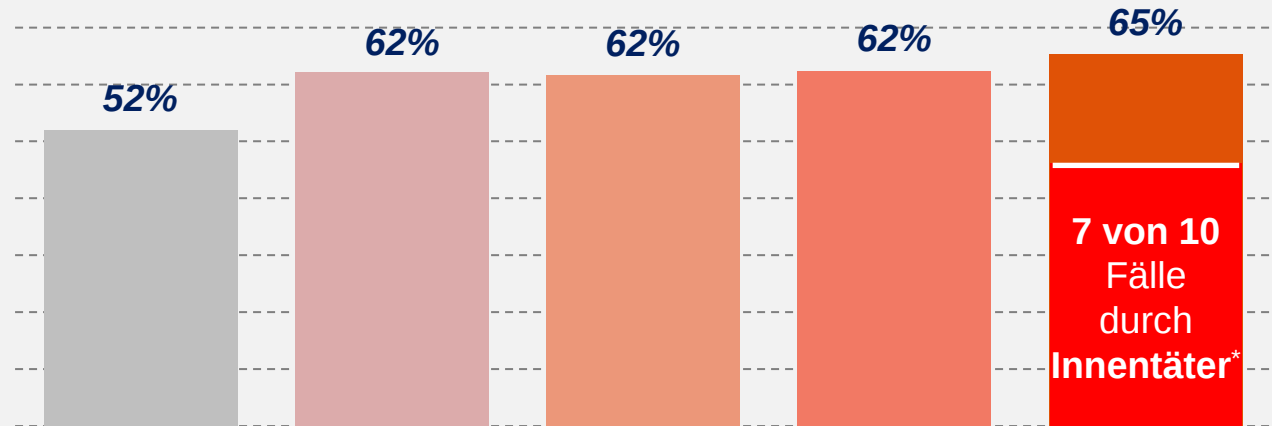
<https://ahaslides.com/RMA23>



Cybersecurity und der Innentäter

Die Anzahl der Informationssicherheitsverstöße steigt jedes Jahr.

Wahrscheinlichkeit, dass eine Organisation von Cybercrime betroffen ist



Innentäter verursachen ca. 70% aller Vorfälle!

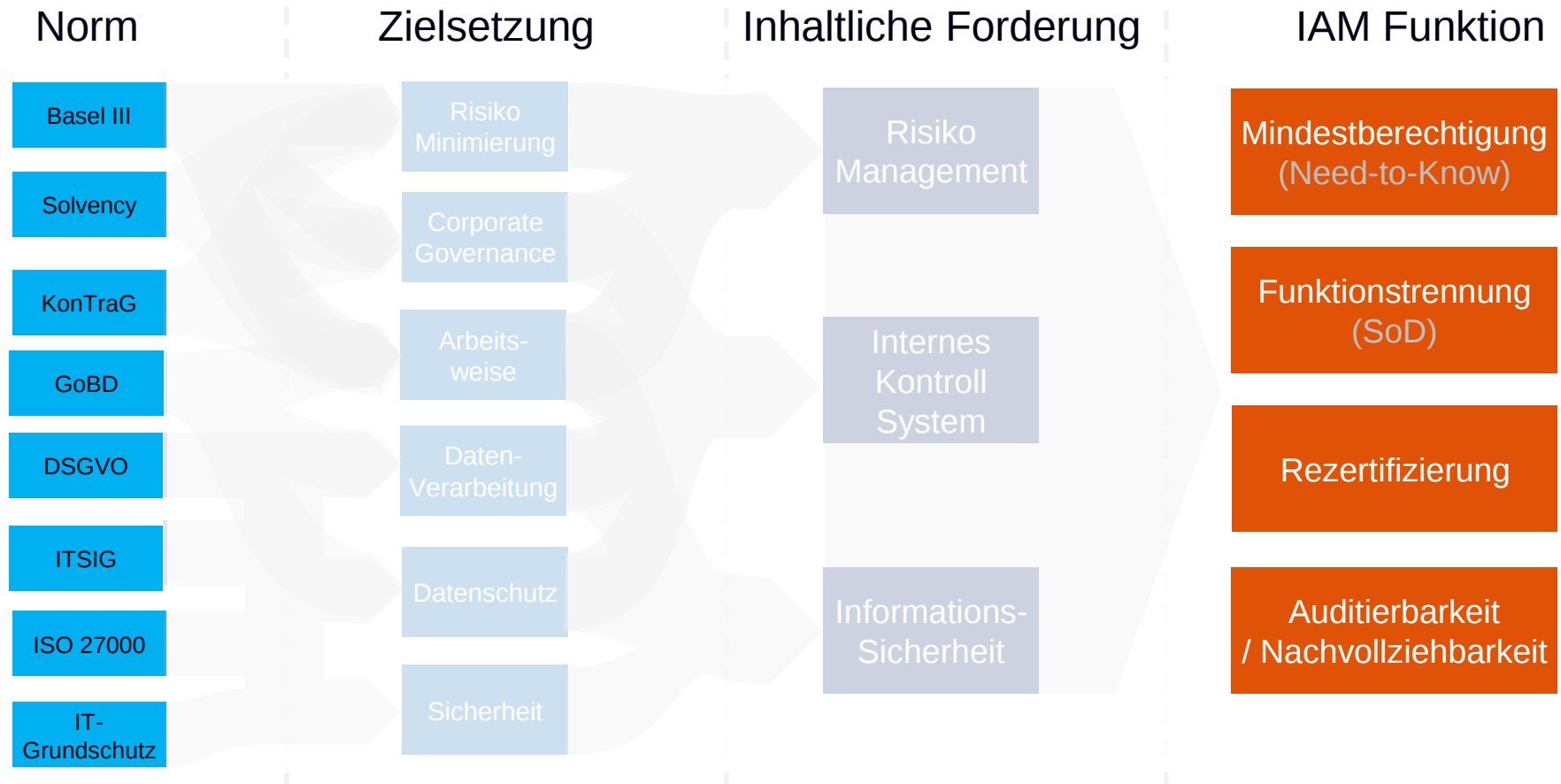
47% Zunahme der Innentäter-basierte Vorfälle seit 2018**

62% der Innentäter-Vorfälle entstehen durch Fahrlässigkeit **

* Bitdefender „Hacked Off“ Study 2019

** Cyberedge Group, Cyberthreat Defense Report 2019

Berechtigungsmanagement und Rechtsnormen



Maßnahmen zum Schutz vor dem Innentäter

Unmittelbarer
Widerruf von
Berechtigungen

Prinzip der
Rollenteilung (SoD)

Geeignete Prozesse
für Mitarbeiter-
Einstellungen

Keine Änderung auf
Zuruf

Vier-Augen-Prinzip
berücksichtigen

Geeignete Prozesse
für Mitarbeiter-
Versetzungen

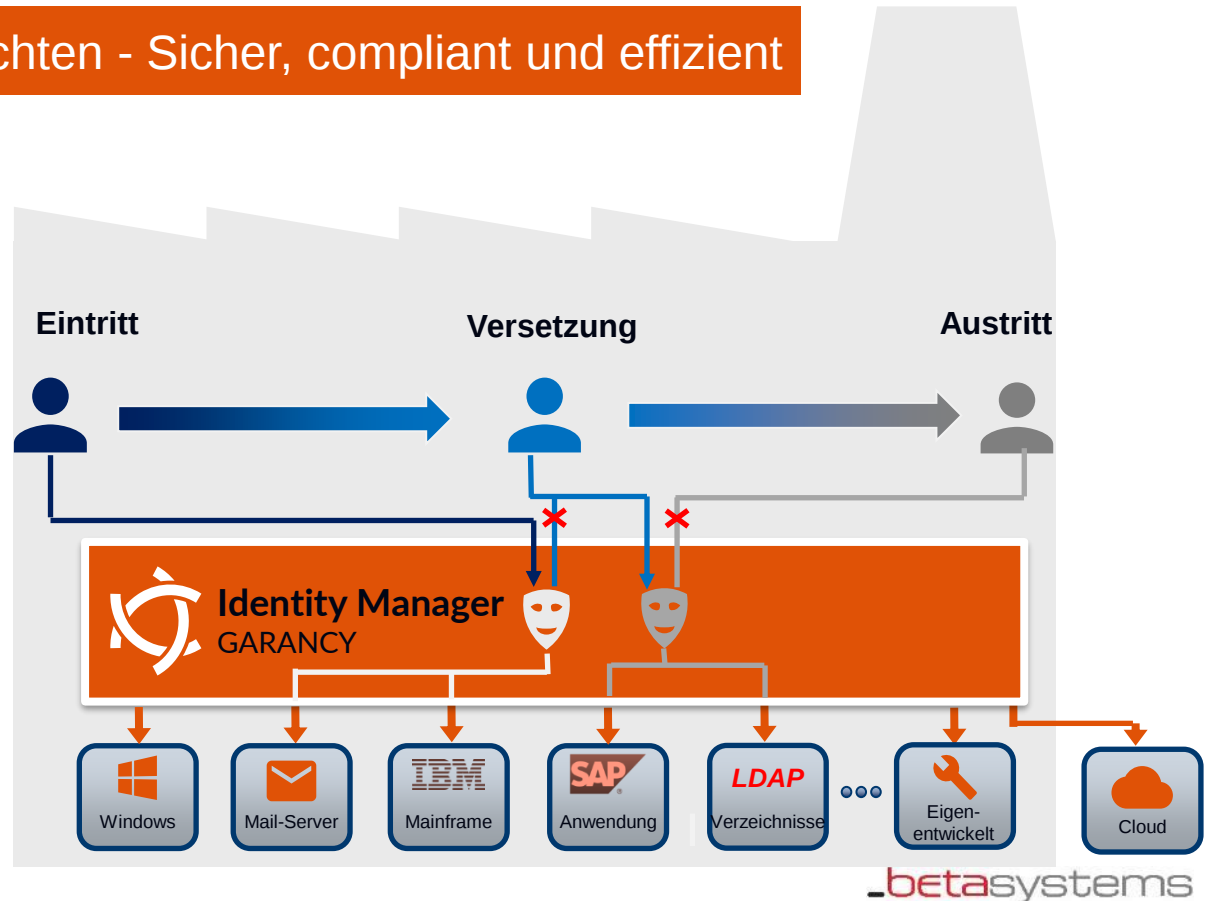
Regelmäßige
Prüfung des
Personals

Geeignete Prozesse
für Mitarbeiter-
Austritte

Garancy Identity & Access Management

Steuerung von Zugangsrechten - Sicher, compliant und effizient

- Verwaltung von Personen und ihrer Berechtigungen entlang ihrer Entwicklung in den Unternehmen.
- Transparenz und Kontrolle der Berechtigungsvergabe zu jedem Zeitpunkt
- Direkte Umsetzung von Berechtigungsentscheidungen in den angeschlossenen Anwendungen



Die beste Vorbeugung – Das Need-to-Know Prinzip

Mitarbeitende erhalten nur die Rechte, die sie für ihre Tätigkeiten brauchen.

PCI-DSS (Payment Card Industry Data Security Standard)

... Beschränken Sie den Zugriff auf Systemkomponenten und Karteninhaberdaten auf diejenigen Personen, deren Tätigkeit einen solchen Zugriff erfordert

HIPAA (Health Insurance Portability and Accountability Act)

... Ein erfasstes Unternehmen muss Richtlinien und Verfahren entwickeln und umsetzen, die den Zugang und die Nutzung von PHI (Protected Health Information) einschränken, basierend auf den spezifischen Rollen der Mitglieder ihrer Belegschaft.

MaRisk -Mindestanforderungen a. d. Risikomanagement (AT 7.2)

... sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt.



Mindestberechtigungsprinzip

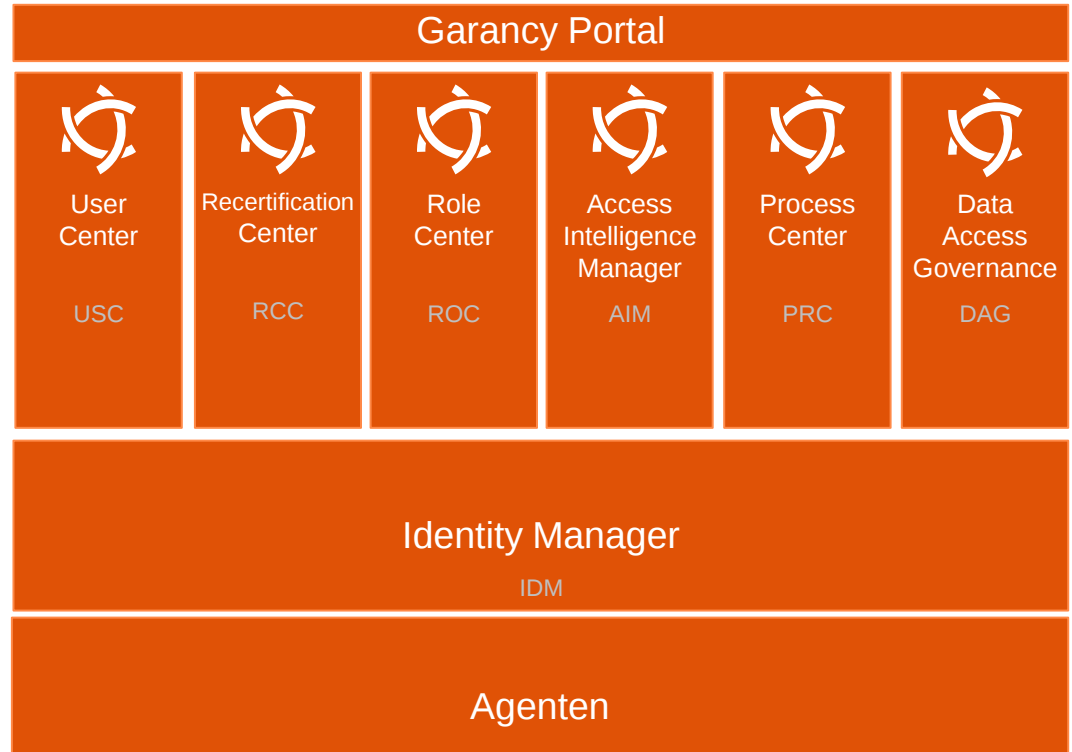
Eine Teamarbeit von Fachabteilung und der IT

Governance durch den Fachbereich

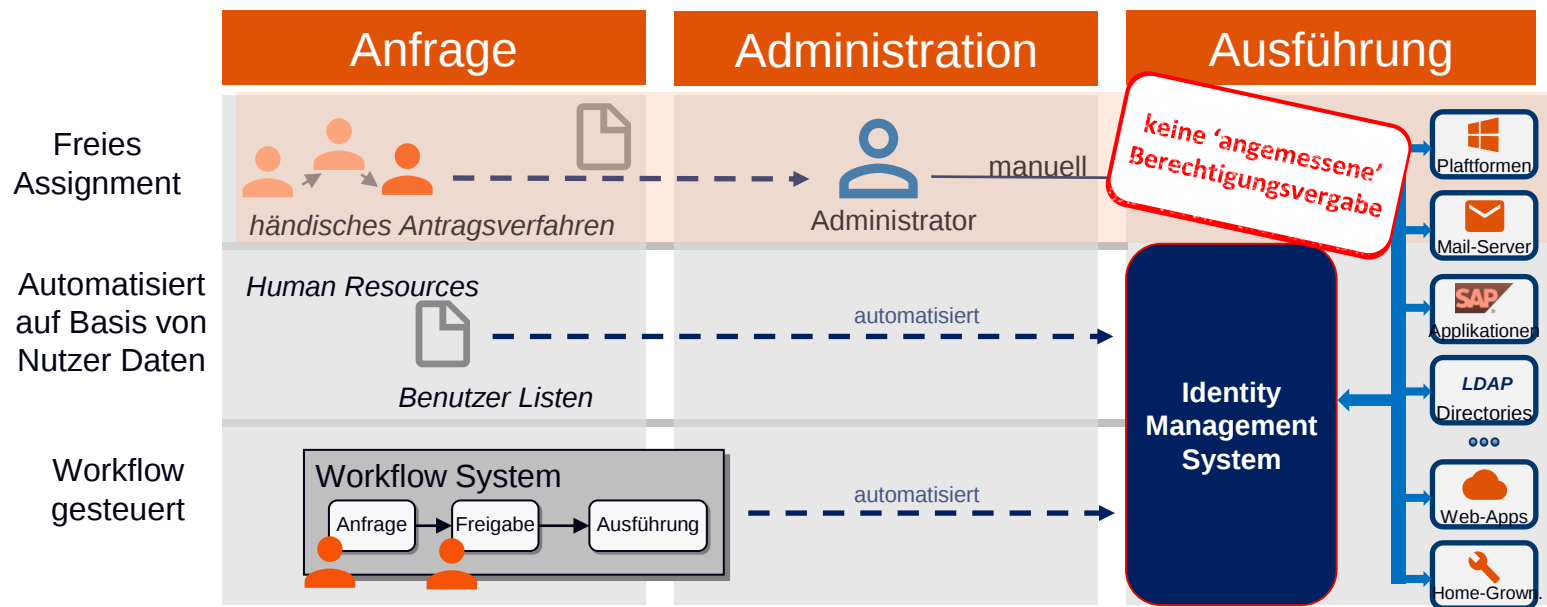
- › Fachliche Bedarfseinschätzung
- › Wissen um mögliche Veränderungen in Aufgaben und Arbeitsumfeld

Provisioning durch die IT

- › Automatisiertes Setzen / Löschen von Berechtigungen
- › Regelbasierte Berechtigungsvergabe



Workflow-gesteuerte Zugriffsregelung bietet Komfort und Compliance



Mitarbeiterereintritt – Automatisierte Verarbeitung

Automatisiertes Berechtigungsmanagement für alle behördenweiten Benutzer

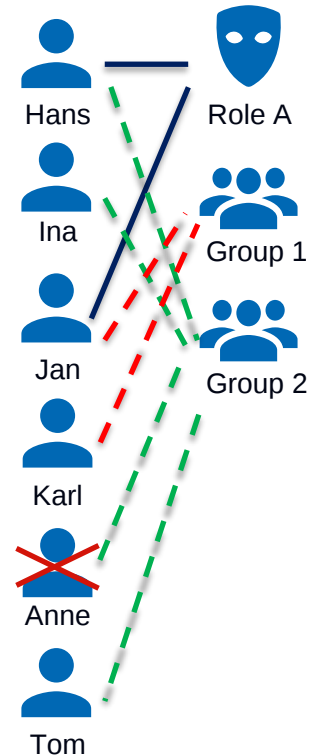
1. Eine Liste aller Benutzer wird periodisch erstellt.
2. Diese 'HR'-Liste wird von Garancy IDM verarbeitet.
3. Basierend auf konfigurierbaren Regeln werden die Benutzer mit Berechtigungen gemäß ihrer Profile ausgestattet.
4. Neue Benutzer werden sofort mit Zugriffsrechten ausgestattet.
5. Ändert ein Benutzer sein Profil, werden die Berechtigungen entsprechend angepasst.
6. Wenn ein Benutzer die Behörde verlässt, werden die Zugriffsrechte entfernt.

#	User	Abteilung	Büro
1	Hans	Vertrieb	Berlin
2	Ina	Personal	Berlin
3	Jan	Vertrieb	München
4	Karl	Finanzen	München
5	Anne	Accounting	Berlin
6	Tom		Bonn Berlin

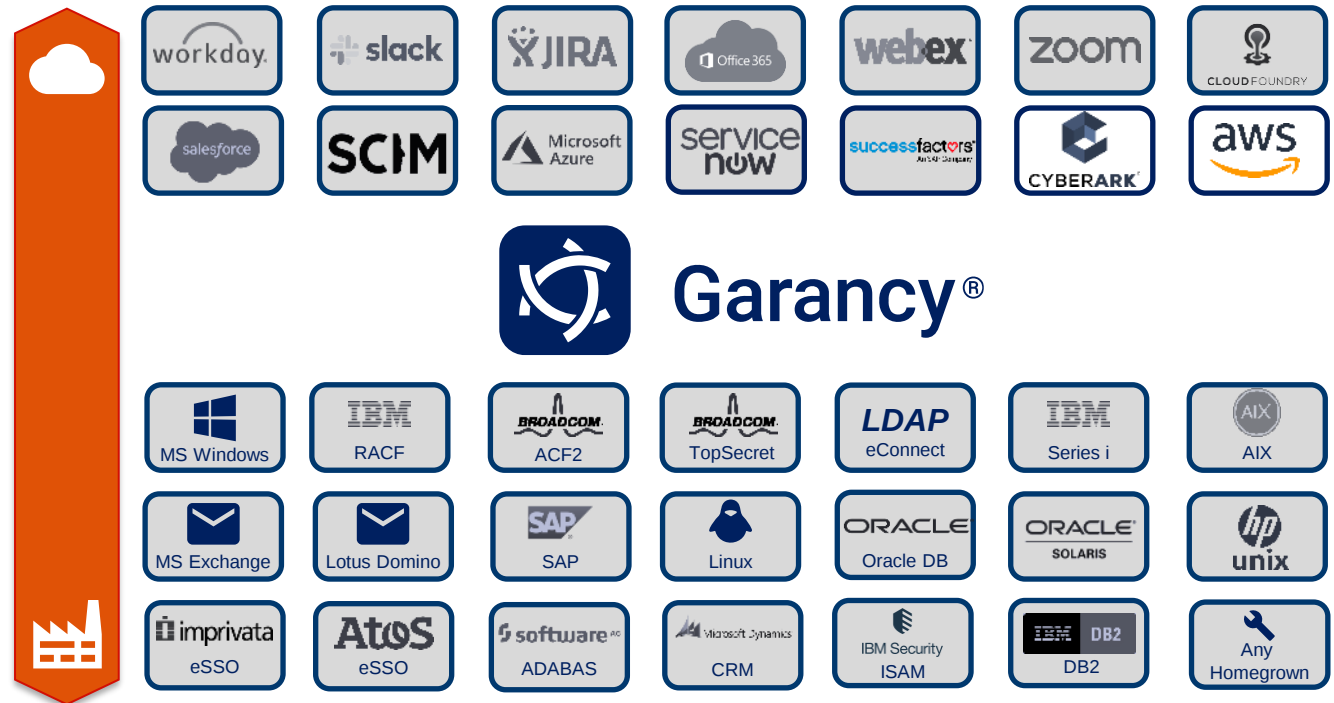
HR Import



```
.....
.....
Vertrieb = Rolle A
München = Group 1
Berlin  = Group 2
.....
.....
```



Getroffene Governance-Entscheidungen zur Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen müssen nachvollziehbar und zeitnah im Zielsystem umgesetzt werden.



Provisionierung – Verschiedene Techniken

Eine sichere und schnelle Umsetzung von Berechtigungsanweisungen kann in Garancy IAM über verschiedene Wege erfolgen:

Standard-Konnektoren

Fertige Anbindung an führende IT-Systeme zur sofortigen Durchführung der Provisionierung

Konnektoren-Frameworks

Konfigurierbare/Anpassbare Konnektorsysteme zur Anbindung individueller Anwendungen an Garancy

Manuelle Provisionierung

Dokumentierte und prüfbare Anweisung von Provisionierungsaufträgen an menschliche Operatoren.



Mitarbeiter Eintritt

Regel- und Antragsbasierte Vergabe von Berechtigungen.



Mitarbeiterversetzung

Anpassung von Zugriffsrechten bei Veränderungen



Individuelle Berechtigungsanforderungen

Auditierbares Antragsverfahren zu jedem Zeitpunkt



Mitarbeiter Rezertifizierung

Periodische Bestätigung von Zugriffsrechten durch den Vorgesetzten.



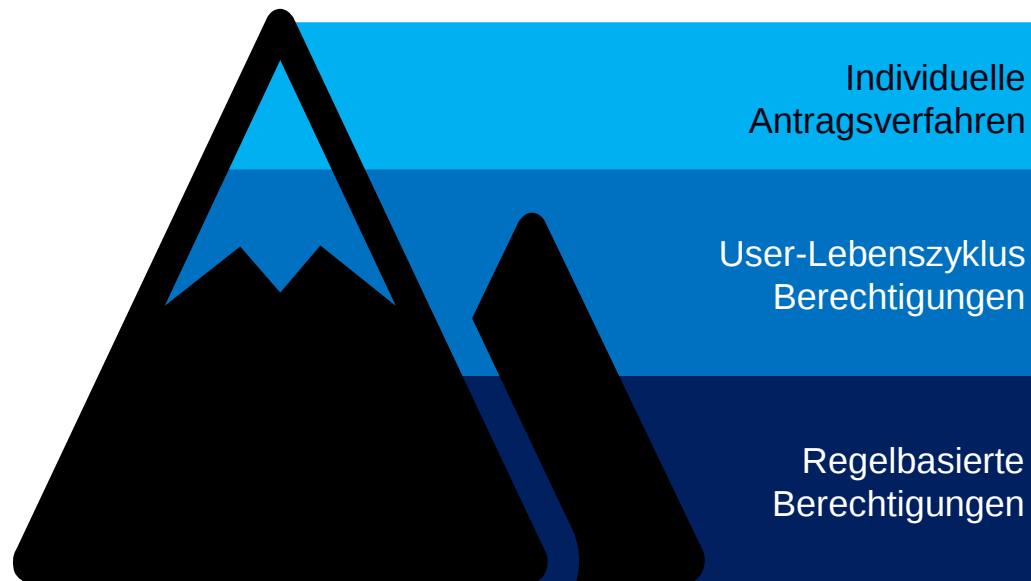
Mitarbeiter Austritt

Automatisierter Entzug bestehender Zugriffsrechte



■ Zuordnung-/Entzug von Berechtigungen (Rollen/Rechte)

- › Die verbleibende Berechtigungen müssen ebenfalls nachvollziehbar und sicher vergeben und entzogen werden.
- › Über die Prozesse zur Steuerung der Benutzerlebenszyklen werden weitere große Mengen an Rechten vergeben.
- › Der Großteil der Berechtigungen wird in vielen Ämtern regelbasiert vergeben.



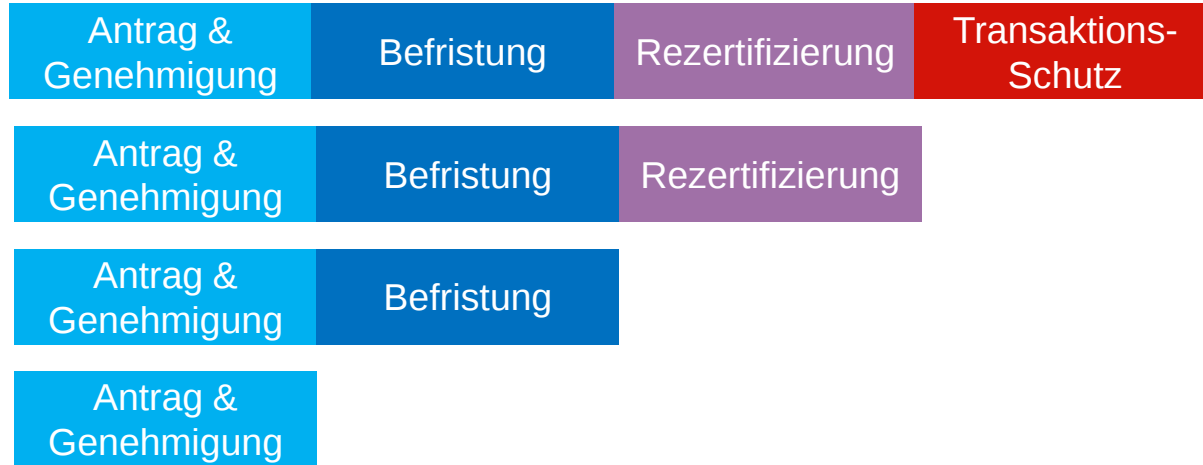
Zero Trust / Vertrauen in getroffene Entscheidungen



Wann wurde
zuletzt geprüft?

Wenn ich niemandem vertraue:

Wie lange vertraue ich dann einer erfolgten Prüfung?



Dauerhafte Entscheidungen

Zero Trust





Risikoreduzierung durch Funktionstrennung

- ...die organisatorische Trennung von Organisationseinheiten oder Stellen im Geschäftsprozess zur Vermeidung von möglichen Interessenkollisionen
- Die Aufbauorganisation muss eine Funktionstrennung zwischen Geschäftsabschluss, Abwicklung und Risikocontrolling haben
- Das Vier-Augen-Prinzip ist das älteste Prinzip der Funktionstrennung. Verhindert werden soll, dass wichtige Entscheidungen von einer einzelnen Person getroffen oder kritische Tätigkeiten von einer einzelnen Person durchgeführt werden

MaRisk

Kreditwesengesetz

Solvency II

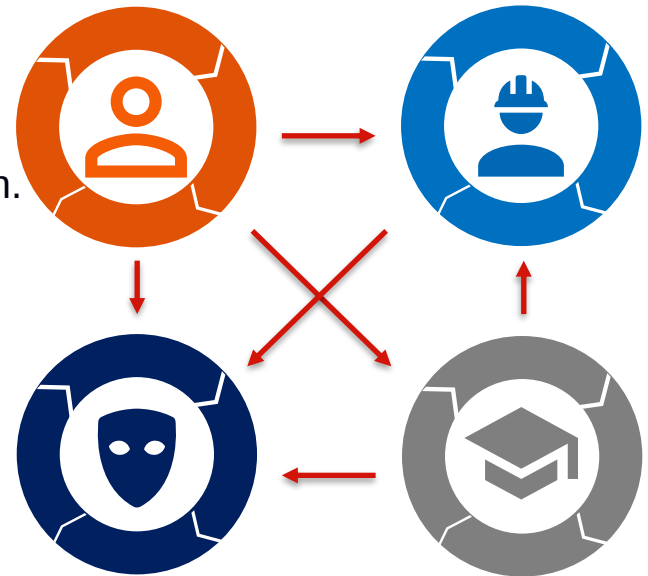
BSI IT
Grundschutz

Rezertifizierung von Anwender Zugriffsberechtigungen

Die Benutzerzugriffsrechte müssen regelmäßig überprüft werden.

- Die Position des Benutzers hat sich möglicherweise geändert.
- Die Aufgaben dieser Position können sich geändert haben.
- Die Inhalte von Rollen können sich geändert haben.
- Die Richtlinien über Berechtigungen können sich geändert haben.

Deshalb sind Rezertifizierungen von Anwendern ein Muss.





Garancy®

Garancy IAM bietet vielfältige Auswertungs- und Berichtsmöglichkeiten für

- Prozessverläufe
- Prozessübersichten
- aktuelle Berechtigungslage
- Veränderungen über die Zeit
- individuelle Abfragen
- uvm.



Zusammenfassung

Unmittelbarer
Widerruf von
Berechtigungen



Prinzip der
Rollenteilung (SoD)



Geeignete Prozesse
für Mitarbeiter-
Einstellungen



Keine Änderung auf
Zuruf



Vier-Augen-Prinzip
berücksichtigen



Geeignete Prozesse
für Mitarbeiter-
Versetzungen



Regelmäßige
Prüfung des
Personals



Geeignete Prozesse
für Mitarbeiter-
Austritte



Zusammenfassung

- ⌘ Es gibt vielfältige Vorschriften und Standards zum Berechtigungsmanagement, die aber inhaltlich große Ähnlichkeiten haben.
- ⌘ Grundlage vieler Normen ist die Informationssicherheit: Vertraulichkeit, Integrität, Verfügbarkeit.
- ⌘ Das Mindestberechtigungsprinzip (Need-to-know) stützt die Informationssicherheit.
- ⌘ Identity & Access Management Systeme helfen bei der Umsetzung des Need-to-Know Prinzips
- ⌘ GARANCY IAM von Beta Systems ist das führende deutsche IAM-System.





...und was können wir für Sie tun?

_betasystems

Niels von der Hude

Director Product Strategy

Beta Systems IAM Software AG Phone +49 – (0)30 726 118 - 0
Alt-Moabit 90d, 10559 Berlin

niels.von-der-hude@betasystems.com
www.betasystems-iam.com

_betasystems