KPMG

Was Sie über Ihr Berechtigungs-management wissen sollten

Nachweisliche Umsetzung regulatorischer Anforderungen

In Kooperation mit

_betasystems

Januar 2019

Inhaltsübersicht

Produktbeschreibung Garancy Access Intelligence Manager (AIM)

Garancy Access Intelligence Manager eröffnet den Zugang zu leistungsstarken Analysefunktionen wie:

- Überwachung unterschiedlichster Datenquellen
- Analyse der aktuellen Zugriffsberechtigungen
- Historische Analyse der Zugriffsberechtigungen durch das Garancy Time-Traveler-Modul
- Forensische Untersuchungen
- Häufigkeits- und Trendanalysen
- Risikoanalysen sowie Analysen für Role-Management
- Erfüllung von Compliance-Anforderungen an die Zugriffsberechtigungen
- die Vermeidung von Identitätsmissbrauch oder Bedrohung durch Insider

Mit diesen Funktionen erhalten Unternehmen tiefen Einblick in ihre Berechtigungslandschaft und deren zugrundeliegende Organisationsstruktur.

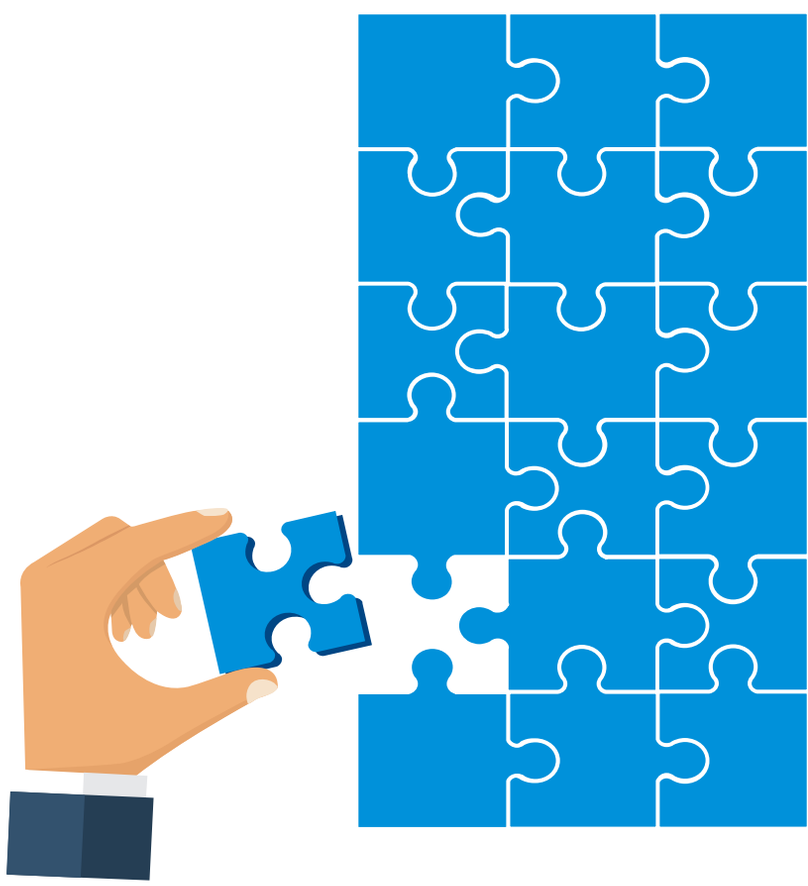
Diese Informationen bilden das Fundament für effektive Governance-Maßnahmen im gesamten Unternehmen, die sich unmittelbar zur Analyse und Aufbereitung der in den User Provisioning-Systemen generierten Daten nutzen lassen.

Die Zugriffsberechtigungen werden zunehmend von den Fachabteilungen im Unternehmen verwaltet. Deshalb stellt der Garancy AIM alle relevanten Benutzerdaten in verständlichen Dashboards zur Verfügung und bietet Analysemöglichkeiten mit nur einem Knopfdruck. Auf diese Weise können Sie insbesondere im Falle eines Audits die Einhaltung interner und externer Anforderungen nachweisen.

Auf Basis eines Data-Warehouse-Systems sammelt und speichert Garancy AIM Berechtigungsdaten und deren Beziehungen untereinander. Dies betrifft insbesondere Änderungen im Status oder der Beziehung zueinander. Die Daten werden in einer multidimensionalen Form gespeichert, sodass erweiterte Auswertungen durchgeführt werden können, die mit einem normalen Reporting-System nicht möglich sind (z. B. historische Auswertungen, Ende-zu-Ende-Betrachtungen, Risikoanalysen oder Compliance-Indikatoren). Im Gegensatz zu den snapshot-basierten Ansätzen wird eine vollständige Historie durch eine kontinuierliche Übernahme der Änderungen ermöglicht, sodass beliebige Zeiträume bis hin zu untertägigen Änderungen vielseitig analysiert werden können.

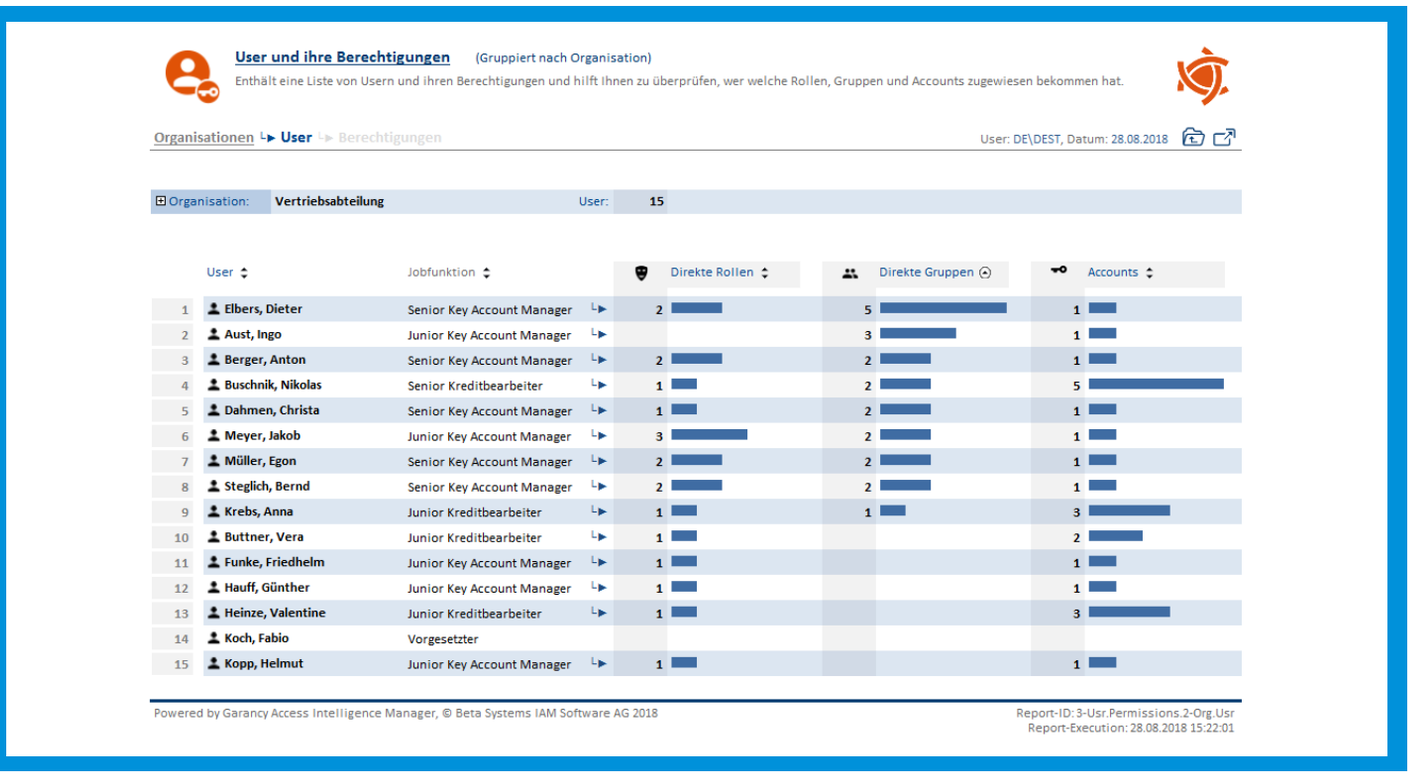
Die Lösung macht Geschäftsabläufe transparent, sicher und auch rückwirkend bewertbar. Sie analysiert sämtliche unternehmensrelevanten Datenquellen und stellt diese in Form von interaktiven Drill-down- und Drill-through-Berichten zur Verfügung.

Das Garancy-AIM-Analysetool kann mit der Garancy AIM Suite oder anderen IAM-Systemen verknüpft werden und bietet damit eine schnelle und effiziente Lösung für weitergehende Analyseoptionen von spezifischen IAM-Daten.



Beispiele von Garancy-AIM-basierten Analysen

Analyse der aktuellen Berechtigungen von Mitarbeitern: Dies erlaubt unter anderem einen Vergleich der Mitarbeiter einer Organisationseinheit bezüglich der Anzahl zugewiesener Berechtigungen, zum Beispiel im Zuge einer Ausreißeranalyse.



User und ihre Berechtigungen (Gruppiert nach Organisation)

Enthält eine Liste von Usern und ihren Berechtigungen und hilft Ihnen zu überprüfen, wer welche Rollen, Gruppen und Accounts zugewiesen bekommen hat.

Organisationen ▸ **User** ▸ Berechtigungen — User: DE\DEST, Datum: 28.08.2018

Organisation: **Vertriebsabteilung** User: **15**

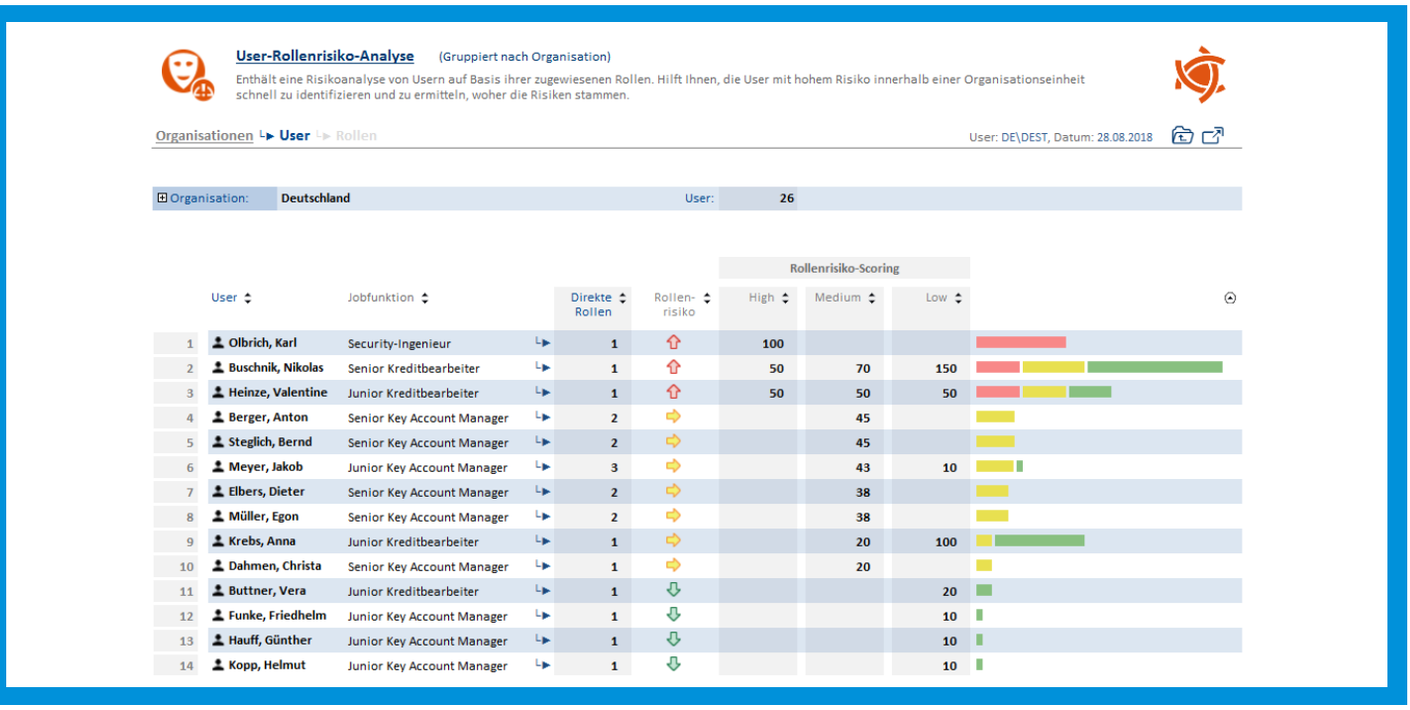
	User	Jobfunktion	Direkte Rollen	Direkte Gruppen	Accounts
1	Elbers, Dieter	Senior Key Account Manager	2	5	1
2	Aust, Ingo	Junior Key Account Manager		3	1
3	Berger, Anton	Senior Key Account Manager	2	2	1
4	Buschnik, Nikolas	Senior Kreditbearbeiter	1	2	5
5	Dahmen, Christa	Senior Key Account Manager	1	2	1
6	Meyer, Jakob	Junior Key Account Manager	3	2	1
7	Müller, Egon	Senior Key Account Manager	2	2	1
8	Steglich, Bernd	Senior Key Account Manager	2	2	1
9	Krebs, Anna	Junior Kreditbearbeiter	1	1	3
10	Buttner, Vera	Junior Kreditbearbeiter	1		2
11	Funke, Friedhelm	Junior Key Account Manager	1		1
12	Hauff, Günther	Junior Key Account Manager	1		1
13	Heinze, Valentine	Junior Kreditbearbeiter	1		3
14	Koch, Fabio	Vorgesetzter			
15	Kopp, Helmut	Junior Key Account Manager	1		1

Powered by Garancy Access Intelligence Manager, © Beta Systems IAM Software AG 2018

Report-ID: 3-Usr.Permissions.2-Org.Usr
Report-Execution: 28.08.2018 15:22:01

Quelle: Beta Systems. Darstellungen basieren nicht auf realen Daten.

Risikoanalyse der aktuell zugewiesenen Rollen innerhalb einer Organisationseinheit sortiert nach dem aufsummierten Risiko:



User-Rollenrisiko-Analyse (Gruppiert nach Organisation)

Enthält eine Risikoanalyse von Usern auf Basis ihrer zugewiesenen Rollen. Hilft Ihnen, die User mit hohem Risiko innerhalb einer Organisationseinheit schnell zu identifizieren und zu ermitteln, woher die Risiken stammen.

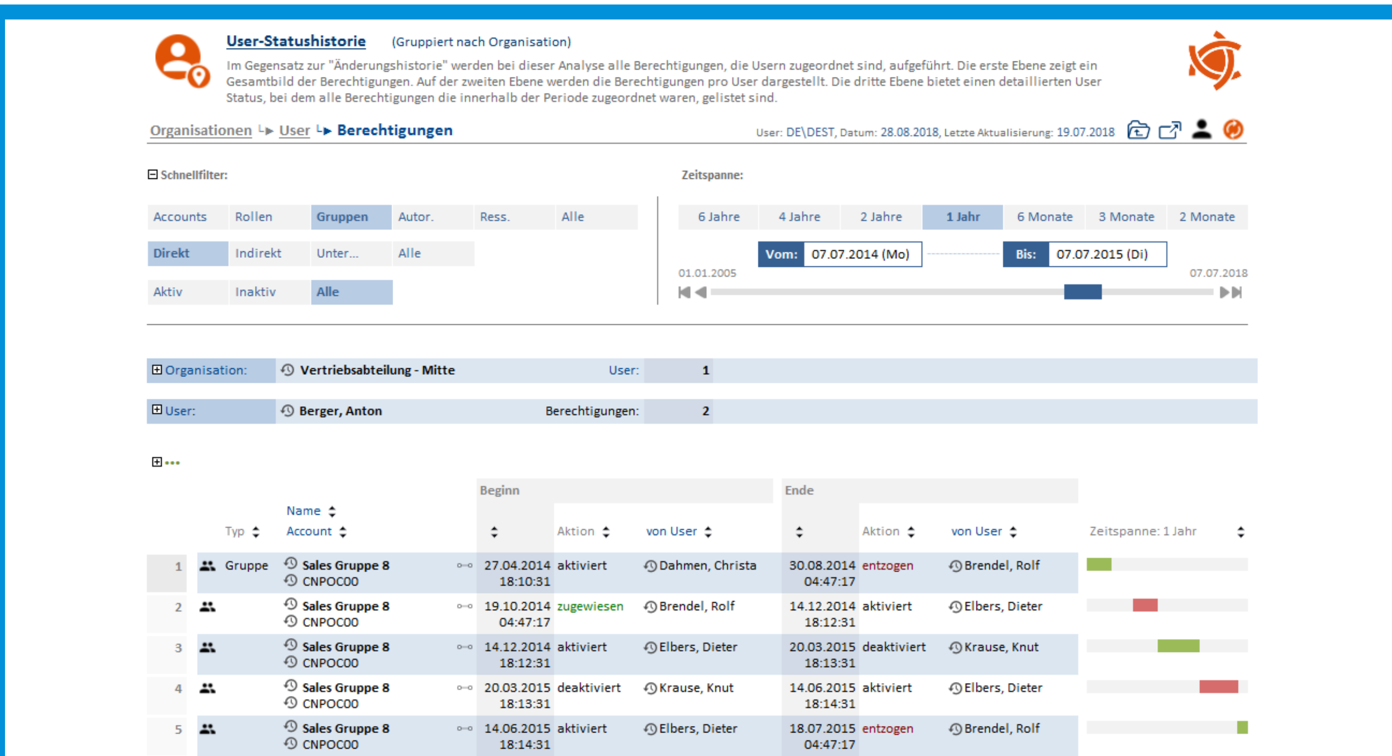
Organisationen ▸ **User** ▸ Rollen — User: DE\DEST, Datum: 28.08.2018

Organisation: **Deutschland** User: **26**

	User	Jobfunktion	Direkte Rollen	Rollen-risiko	Rollenrisiko-Scoring: High	Medium	Low
1	Olbrich, Karl	Security-Ingenieur	1	⇧	100		
2	Buschnik, Nikolas	Senior Kreditbearbeiter	1	⇧	50	70	150
3	Heinze, Valentine	Junior Kreditbearbeiter	1	⇧	50	50	50
4	Berger, Anton	Senior Key Account Manager	2	⇨		45	
5	Steglich, Bernd	Senior Key Account Manager	2	⇨		45	
6	Meyer, Jakob	Junior Key Account Manager	3	⇨		43	10
7	Elbers, Dieter	Senior Key Account Manager	2	⇨		38	
8	Müller, Egon	Senior Key Account Manager	2	⇨		38	
9	Krebs, Anna	Junior Kreditbearbeiter	1	⇨		20	100
10	Dahmen, Christa	Senior Key Account Manager	1	⇨		20	
11	Buttner, Vera	Junior Kreditbearbeiter	1	⇩			20
12	Funke, Friedhelm	Junior Key Account Manager	1	⇩			10
13	Hauff, Günther	Junior Key Account Manager	1	⇩			10
14	Kopp, Helmut	Junior Key Account Manager	1	⇩			10

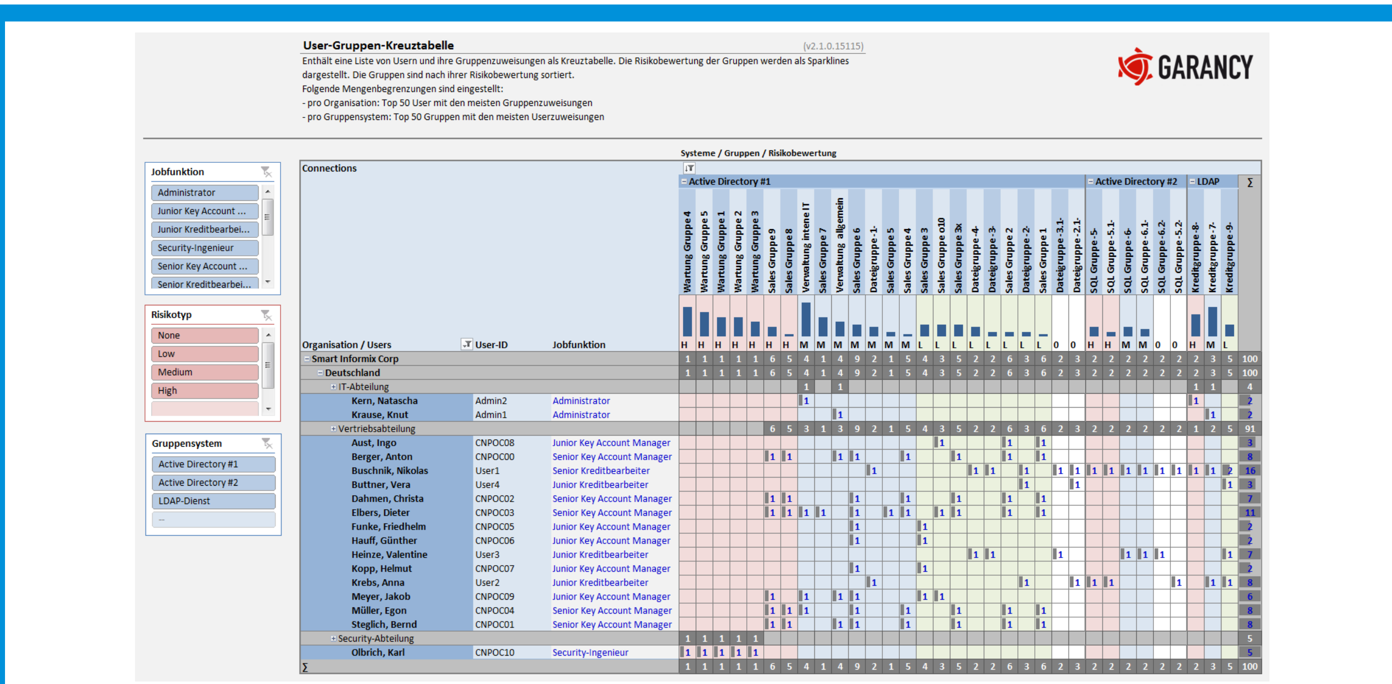
Quelle: Beta Systems. Darstellungen basieren nicht auf realen Daten.

Historienanalyse der zugewiesenen Gruppen eines Users in einem bestimmten Zeitraum (Gantt-Darstellung):



Quelle: Beta Systems. Darstellungen basieren nicht auf realen Daten.

Beispiel einer Ad-hoc-Analyse der Benutzer und der ihnen zugeordneten Gruppen in Form einer Kreuztabelle in Excel.



Quelle: Beta Systems. Darstellungen basieren nicht auf realen Daten.

Äußere Rahmenbedingungen

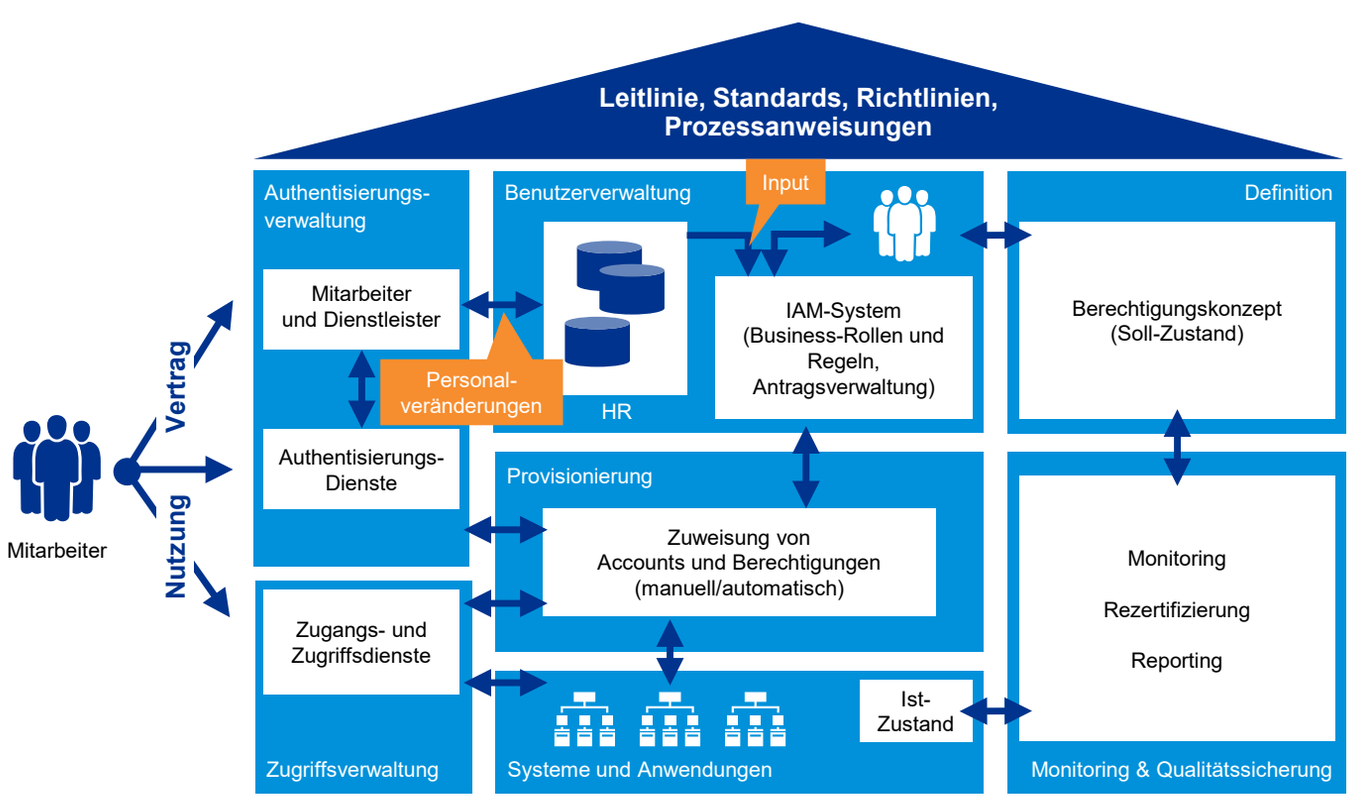
Viele Unternehmen, vorwiegend im Finanzsektor, unterliegen strengen regulatorischen Anforderungen. Insbesondere sind dies die MaRisk (Rundschreiben 09/2017 (BA) vom 27.10.2017) und die BAIT (Rundschreiben 10/2017 (BA) vom 03.11.2017). Auch andere Sektoren sind zumindest vom Gesetzgeber getrieben (z. B. über BDSG oder DSGVO) oder lehnen sich an verschiedene Standards an (z. B. ISO/IEC 27001 oder COBIT), um die IT im eigenen Haus zu schützen. Darunter fallen seit 2015 auch Unternehmen mit kritischen Infrastrukturen, für die die die BSI-Kritisverordnung gilt. Das Thema Identity und Access Management, findet in all den eben genannten Anforderungen Bedeutung. Dabei wird zum Beispiel in der MaRisk AT 4.3.1 Tz. 1 das Thema der Funktionstrennung genau definiert und in der BAIT 24 der Umgang mit Berechtigungskonzepten.

Damit diese Vorgaben auch eingehalten werden, werden Unternehmen extern oder von der eigenen Revision geprüft. In diesem Kontext ist es hilfreich, gezielte Audit-Analysen vorweisen zu können, um eine schnelle Datenlieferung im Rahmen einer Prüfung erfüllen zu können und damit die Einhaltung von Compliance-Anforderungen nachweisen und gegebenenfalls Abweichungen dokumentieren zu können.

Um diesen Anforderungen und somit den Zielen des Berechtigungsmanagements (Compliance, Sicherheit und Effizienz) gerecht zu werden, ist technische Unterstützung von Vorteil. Die Anschaffung eines Tools zur automatisierten Umsetzung verschiedener Prozesse im Berechtigungsmanagement alleine reicht dazu nicht aus. Es müssen auch die entsprechenden Prozesse und Vorgaben (fachlich/technisch) definiert und umgesetzt sein.

Die KPMG AG Wirtschaftsprüfungsgesellschaft (KPMG) ist dabei als Dienstleister für Identity and Access Management (IAM) Ihre erste Wahl, denn das Unternehmen verfügt über umfangreiche Projektmanagement-Erfahrung sowie eine breite Fach- und Architektur-Kompetenz – spezifisch zugeschnitten auf das Thema Berechtigungsmanagement. Dies gibt die erforderliche Sicherheit bei der Operationalisierung und Realisierung der Aufgabenstellungen im Berechtigungsmanagement. Die Komplexität des Themenfelds zeigt sich in der folgenden Darstellung:

Komplexität im Berechtigungsmanagement



Quelle: KPMG Deutschland, 2019

Folgende Feststellungen ergeben sich bei externen oder internen Prüfungen immer wieder und beschreiben damit den aktuellen Handlungsbedarf für Unternehmen im Themenfeld Berechtigungsmanagement:

- Intransparenz der vergebenen bzw. benötigten Berechtigungen (z. B. fehlende Reporting-möglichkeiten oder Qualität der Berechtigungs-beschreibungen)
- Intransparenz auf „Legalisierungen“ (Anträge/Freigaben nicht nachvollziehbar)
- Überberechtigungen (z. B. „Azubi-Effekt“ oder in Bezug auf privilegierte Accounts)
- Verstöße gegen Funktionstrennungsvorgaben aufsichtsrechtlicher Art (insbesondere MaRisk bei Finanzinstituten) oder interner Art (z. B. im Einkaufsverfahren)
- Berechtigungsprobleme bei einzelnen Systemen, vor allem, SAP, Active Directory, Filesystem, Sharepoints, aber auch Anwendungen u. a.
- Ineffiziente und unübersichtliche Antragsverfahren (z. B. uneinheitlich oder ohne echte Systematik, Referenz-User-basierend)
- Dauer und Aufwand der Bearbeitung bei manueller Berechtigungsvergabe/-löschung
- Keine periodische Qualitätssicherung („Rezertifizierung“)
- Mangelnde Akzeptanz von Verantwortung
- Ausfall- und Wartezeiten bei IT-Systemen
- Umgang mit www-Berechtigungen (z. B. bezüglich Informationseigentümer, Erfassung in CMDB)
- Überlastung des Service Desks durch steigende Vielfalt der Anwendungslandschaft und sich wiederholender Standardanfragen
- Überblick über externe Mitarbeiter/Dienstleister und deren Zugriffe auf Unternehmensdaten nicht vorhanden/unvollständig
- Berechtigungen nicht nach Businessfunktionen organisiert, kein Rollenmodell vorhanden

Um aufzuzeigen, wie die technische Lösung Garancy AIM als Analysetool von Beta Systems und die fachliche Kompetenz von KPMG bei solchen Feststellungen effiziente Lösungen erbringen können, werden nachfolgend einige beispielhafte Feststellungen vorgestellt und analysiert.

Für die Nutzung des Garancy AIM ist es sehr empfehlenswert, ein IAM-System (Identity and Access Management) zu verwenden. Dieses kann dann mit dem Analysetool Garancy AIM verbunden werden. Als Beispiel für ein IAM-System soll kurz das von Beta Systems entwickelte Produkt Garancy IAM Suite vorgestellt werden.

Mit der Garancy Identity Access Management Suite von Beta Systems steuern und überwachen Unternehmen den Zugriff auf Daten und Anwendungen gemäß der individuellen organisatorischen Anforderungen und fachlichen Rolle eines jeden Benutzers.

Die Module der Beta Systems IAM Suite bedienen alle Aufgaben von Identity Access Governance und sind sowohl in der Cloud als auch lokal im eigenen Rechenzentrum verfügbar:

Garancy IAM Suite von Beta Systems

Quelle: Beta Systems

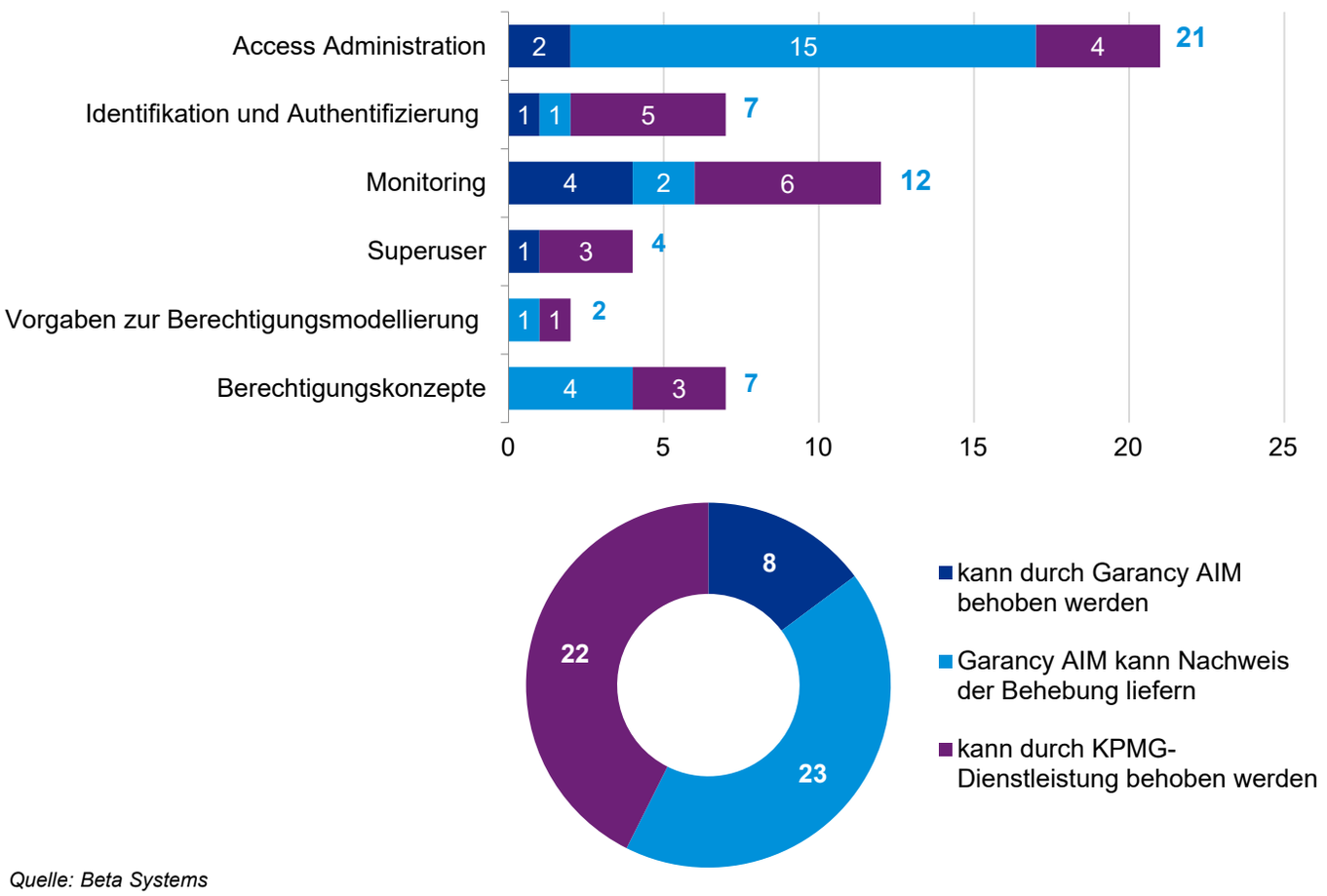
Untersuchte Feststellungen im Berechtigungs-management

KPMG als Kooperationspartner von Beta Systems hat die selbst ermittelten und im Rahmen von Projekten bearbeiteten Feststellungen im Bereich des Berechtigungsmanagements untersucht. Als Feststellung ist im Folgenden eine Abweichung von bindenden internen oder externen Anforderungen zu verstehen.

Dabei hat sich herausgestellt, dass ein Anteil von 15% der Feststellungen direkt durch die Analyse- und Report-Möglichkeiten des Garancy AIM behoben werden kann. Zudem kann Garancy AIM bei mehr als der Hälfte der Feststellungen bei der Behebung unterstützen, zum Beispiel durch Erstellung von Nachweisen. Insgesamt kann somit Garancy AIM für mehr als die Hälfte aller Feststellungen Lösungen bzw. Unterstützung anbieten. Auch zur Eigenkontrolle und zur Vorbereitung von Auditierungen eignet sich Garancy AIM. Ebenso kann Garancy AIM bei der Dokumentation der Berechtigungsstrukturen in den grundlegenden Konzepten unterstützen und deren Umsetzung nachweisen. Identifizierte Feststellungen, die keinen Bezug zu Garancy AIM haben und wo Garancy AIM nicht zum Einsatz kommt, können mit Dienstleistungen von KPMG unterstützt werden.

Die insgesamt 53 ermittelten Feststellungen wurden in sechs Kategorien eingeordnet, um diese thematisch zu clustern. Die Kategorien ergeben sich aus einem KPMG-Prüfleitfaden. In diesem Dokument sind beispielhaft allgemeine IT-Kontrollen sowie IDW PS 330 Application Controls, Prüfungshandlungen zur Aufbau- und Funktionsprüfung, häufige IT-Feststellungen, mögliche Auswirkungen dieser Feststellungen auf Anwendungskontrollen sowie mögliche ergänzende Prüfungshandlungen beschrieben. Sie stellen typische IT-Kontrollen dar, die jedoch abhängig von der Komplexität und der Risikoeinschätzung für einzelne Mandanten unterschiedlich ausgestaltet sein können. Einzelne Feststellungen lassen sich mehreren Kategorien zuordnen. In diesem Fall ist die Kategorie mit der größeren Schnittmenge gewählt worden.

Feststellungen pro Kategorie



Quelle: Beta Systems

Beschreibung der verwendeten Kategorien

1. Access Administration

Die Kategorie Access Administration umfasst die grundlegenden Aufgaben des Berechtigungsmanagements. Zu diesen Aufgaben zählen die Rezertifizierung von Zugängen und die Umsetzung der Prinzipien der minimalen Berechtigungsvergabe und der Funktionstrennung. Das umfasst sowohl zeitliche Aspekte bezüglich der Prozessdauer, als auch formale Aufgaben hinsichtlich Dokumentation und Autorisierung von Berechtigungsprozessen. Solche Prozesse behandeln im Regelfall die Vergabe, die Änderung oder den Entzug von Berechtigungen.

Häufige Feststellungen resultieren aus einem fehlenden Antragsverfahren, einer unzureichenden Aktualisierungsspanne von Berechtigungen oder der Missachtung eines oder mehrerer der genannten Prinzipien.

Die daraus resultierenden Risiken gefährden direkt die Integrität und Vertraulichkeit von geistigem Eigentum des Unternehmens. Beispielsweise könnte eine überberechtigte Person Unternehmensdaten veruntreuen (beabsichtigt oder unbeabsichtigt) oder mutwillig Daten zum Schaden des Unternehmens manipulieren.

2. Identifikation und Authentifizierung

In den Bereich der Identifikation und Authentifizierung fallen die Vergabe von eindeutig zuordenbaren Identitäten, die Entwicklung, Etablierung und Umsetzung von Richtlinien für Kennwörter und die Überwachung von technischen Benutzerkonten.

Typische Feststellungen finden sich bei einem unvollständigen Überblick über externe Mitarbeiter, bei der mangelnden Zuordnung von Verantwortlichkeiten für technische Benutzerkonten oder bei den Anforderungen bzw. den Umsetzungen von Kennwortrichtlinien.

Eine Missachtung oder Nichterfüllung der entsprechenden Anforderungen aus dem Bereich gefährdet alle drei grundlegenden IT-Schutzziele Integrität, Verfügbarkeit und Vertraulichkeit. Die Unzugänglichkeit von Unternehmensdaten und geistigem Eigentum kann nicht mehr sichergestellt werden. Eine Manipulation, Vernichtung oder Verbreitung der gesamten oder eines Teils der Daten ist möglich.

3. Monitoring

Die Kategorie Monitoring überwacht die Aktivitäten von vergebenen Berechtigungen. Außerdem wird hier geprüft, ob eine systemseitige Funktionstrennung implementiert ist. Regelmäßige Verstöße resultieren aus den Anforderungen an ein dokumentiertes Verfahren, aus der Überwachung von kritischen Berechtigungen oder bei der Erstellung von historischen Reports.

Die Überwachung und Überprüfung der Umsetzung von IT-Sicherheitsrichtlinien dient direkt der Umsetzung der Schutzziele. Ohne Monitoring sind sowohl unentdeckter Missbrauch als auch eine Aufweichung bzw. Umgehung von notwendigen Richtlinien möglich.

4. Superuser

Für die Etablierung eines Superusers ist ein Monitoring der Aktivität und ein Freigabeprozess für das Aufheben von Sicherheits-einstellungen mit einer sauberen Dokumentation notwendig. Außerdem darf lediglich ein kleiner Personenkreis Superuser-Berechtigungen besitzen oder Zugriff auf Mehrbenutzer-Accounts mit Superuser-Berechtigungen haben.

Diese Kontrollen und Einschränkungen sollen das Unternehmen vor unkontrollierten Einzelpersonen mit weitreichenden Befugnissen schützen. Ein mögliches Risiko resultiert aus der Möglichkeit der unkontrollierten Manipulation, Veruntreuung oder Vernichtung von unternehmenskritischen Informationen und Daten durch eine hochberechtigte, unüberwachte Einzelperson.

5. Vorgaben zur Berechtigungsmodellierung

Bei der Modellierung des Berechtigungsmanagements müssen gegebenenfalls staatliche und branchenspezifische Vorgaben, aber auch unternehmenseigene Regelungen eingehalten werden. In diesen Bereich fällt auch die Entwicklung von Business-Rollen, bei denen insbesondere auf die Einhaltung der Funktionstrennung zu achten ist.

Diese Vorgaben dienen dazu sicherzustellen, dass nicht gewollt oder ungewollt unpassende Zugriffsrechte vergeben werden.

6. Berechtigungskonzepte

In den Berechtigungskonzepten muss dokumentiert werden, wer auf welche Daten und IT-Systeme welche Zugriffsberechtigungen besitzt.

Diese Dokumentation dient der Festhaltung und Überprüfung des Berechtigungsmanagements. Es sollen dabei falsch vergebene Berechtigungen und Unterschiede zwischen dem definierten Soll-Zustand und dem tatsächlich vergebenen Ist-Zustand des Berechtigungsmanagements aufgedeckt und behoben werden.

Bewertung der einzelnen Feststellungen nach Kategorien bezogen auf die Auditierung

Die aufgestellten Feststellungen können entweder direkt durch den Einsatz von Garancy AIM behoben oder unterstützt werden oder sind über fachliche Prozesse und Implementierungen lösbar – mit oder ohne Nachweismöglichkeit der Behebung mithilfe von Garancy AIM.

In den nachfolgenden Tabellen werden die behebbaren Feststellungen mit ihrer Bewertung, den resultierenden Risiken oder einem möglichen Lösungsansatz dargestellt. Am Ende einer jeden Kategorie befindet sich eine Auswertung mit Fazit.

Die Risikobeschreibung orientiert sich an den drei grundlegenden IT-Sicherheitszielen Integrität, Verfügbarkeit und Vertraulichkeit. Jede Feststellung verletzt eines oder mehrere der drei genannten Schutzziele. Aus einer Zuordnung zu einem oder mehreren der Schutzziele lässt sich keine Bedeutung oder Gewichtung des Gesamtrisikos ableiten.

1. Access Administration

1.1 Mitarbeiterwechsel/-austritt – keine ausreichenden Prüfungen

Einordnung

Problem	Es werden keine zeitnahen Prüfungen für die manuelle Rücknahme oder Anpassung der Zugriffsrechte von Mitarbeitern, die das Unternehmen verlassen oder die Position innerhalb des Konzerns gewechselt haben, durchgeführt. Nach der MaRisk AT 4.3.1 Tz. 2 müssen Berechtigungen und Kompetenzen nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) vergeben werden und bei Bedarf zeitnah angepasst werden. Nach der ISO 27001 A.9.2.5 sollten Nutzerberechtigungen regelmäßig überprüft werden.
Risiko	Ohne eine regelmäßige Überprüfung der Berechtigungen, insbesondere für Mitarbeiter, die ihre Position wechseln oder das Unternehmen verlassen, besteht das Risiko, dass unberechtigte Zugriffe möglich sind und gegebenenfalls nicht erkannt werden. Sowohl die Vertraulichkeit als auch die Integrität der Unternehmensdaten können nicht mehr sichergestellt werden.
Lösung	Es kann beispielsweise ausgewertet werden, wie sich Berechtigungen von Benutzern aufgrund der Änderung ihrer Jobfunktion verändert haben. Dies kann zum Beispiel in Form eines Zeitstrahls (ähnlich einer Gantt-Darstellung) pro Benutzer ausgewertet werden. Betroffene Benutzer können über die Attributshistorie ermittelt werden.

Kann durch Garancy AIM behoben werden

1.2 Transparenz: Mangelnde Übersicht über aktuelle Berechtigungen von Benutzern

Einordnung

Problem	Es ist nur mit unverhältnismäßig hohem Aufwand möglich zu ermitteln, welche Berechtigungen ein Mitarbeiter besitzt und wer diese genehmigt hat. Nach der BAIT 28 ist die Einrichtung, Änderung, Deaktivierung sowie Löschung von Berechtigungen und deren Rezertifizierungen nachvollziehbar und auswertbar zu dokumentieren.
Risiko	Die fehlende Verantwortlichkeit und Nachvollziehbarkeit für und von Berechtigungen bergen das Risiko, dass das Prinzip der minimalen Berechtigungsvergabe nicht mehr umgesetzt wird. Durch diese Überberechtigung wird das Risiko eines Verstoßes hinsichtlich Vertraulichkeit und Integrität der Unternehmensdaten erhöht.
Lösung	Ein Teil der Feststellung kann durch Garancy AIM direkt behoben werden. Es kann ausgewertet werden, welche Berechtigungen ein Mitarbeiter besitzt (mit einer Zeitleisten-Funktion, die Änderungen sichtbar macht) bzw. welche Mitarbeiter eine bestimmte Berechtigung besitzen. In der Roadmap ist vorgesehen, dass in einer zukünftigen Version auch ausgewertet werden kann, wer jeweils die Genehmigungen erteilt hat.

Kann durch Garancy AIM behoben werden

1.3 Mitarbeiterversetzung – fehlende Festlegung bezüglich Berechtigungsentzug

Einordnung

Problem	Es wurde nicht festgelegt, wie lange frühere Zugriffsrechte nach einem Positionswechsel maximal aufrechterhalten werden dürfen. Nach der MaRisk AT 7.2 Tz. 2 muss die Berechtigungsvergabe sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt. Nach der ISO 27001 A.9.2.3 sollte die Reservierung von privilegierten Berechtigungen kontrolliert und eingeschränkt werden.
Risiko	Um das Prinzip der minimalen Berechtigungsvergabe zu wahren, sind angemessene Fristen für die Rücknahme von Zugriffsrechten notwendig. Je nach Art des Positionswechsels kann sich bei auch nur temporärer Beibehaltung der bestehenden Berechtigungen ein Verstoß gegen Funktionstrennungs-kriterien ergeben. Durch die Verletzung des Prinzips erhöht sich das Risiko, dass die Vertraulichkeit oder die Integrität der Unternehmensdaten verletzt wird bzw. bei Verstoß gegen Funktionstrennungskriterien können ein finanzieller oder regulatorischer Schaden bzw. eine Rufschädigung eintreten.
Lösung	Es kann überprüft werden, wie sich Berechtigungen von Benutzern aufgrund der Änderung ihrer Jobfunktion verändert haben. Dies kann zum Beispiel in Form eines Zeitstrahls (Gantt-Darstellung) pro Benutzer ausgewertet werden.

Garancy AIM kann Nachweis der Behebung liefern

1.4 Mitarbeiteraustritt – keine Kontensperrung

Einordnung

Problem	Benutzerkonten von Mitarbeitern, die das Unternehmen verlassen haben, werden nicht (durchgehend) gelöscht oder gesperrt. Nach der MaRisk AT 4.3.1 Tz. 2 und AT 7.2 Tz. 2 darf jeder Mitarbeiter nur über die Rechte verfügen, die er für seine Tätigkeit benötigt. Berechtigungen und sonstige eingeräumten Kompetenzen sind innerhalb einer angemessen Frist – regelmäßig und anlassbezogen – zu überprüfen. Nach der BAIT 26 ist sicherzustellen, dass die Verfahren zur Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen die Vorgaben des Berechtigungskonzepts einhalten. Nach der ISO 27001 A.9.2.6 sollten die Zugriffsrechte bei Beendigung oder Änderung des Arbeitsverhältnisses, des Vertrags oder der Vereinbarung entfernt oder angepasst werden.
Risiko	Inaktive Benutzerkonten behindern und erschweren das Berechtigungs-management unnötig. Unberechtigte und aktive Benutzerkonten, die noch Zugriff auf Unternehmensdaten haben, gefährden die Vertraulichkeit und Integrität dieser Daten und bergen das Risiko, das über diese Transaktionen durchgeführt werden, die keinem Verursacher zugeordnet werden können.
Lösung	Es kann ein Nachweis generiert werden, der die Sperrungen und Löschungen der Benutzerkonten ehemaliger Mitarbeiter aufzeigen kann. Bei Bedarf kann auf diese Weise auch ausgewertet werden, welche Zeitspanne im Schnitt oder im Maximalfall bis dahin vergangen ist.

Garancy AIM kann Nachweis der Behebung liefern

1.5 Berechtigungskonzept – fehlt für konzernübergreifende Zugriffsrechte

Einordnung

Problem	Es existiert kein konzernübergreifendes Zugriffsrechte-Konzept, sodass das Prinzip der minimalen Berechtigungsvergabe nicht sichergestellt werden kann. Nach der MaRisk AT 4.3.1 Tz. 2 sind Prozesse mit ihren verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswegen klar zu definieren. Berechtigungen und Kompetenzen sind nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) zu vergeben und anzupassen. Nach der BAIT 24 sind der Umfang und die Nutzungsbedingungen der Berechtigungen durch Berechtigungskonzepte festzulegen. Berechtigungskonzepte haben die Berechtigungsvergabe nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) sicherzustellen.
Risiko	Ohne ein zentrales und konzernübergreifendes Zugriffsrechtemanagement kann nicht sichergestellt werden, dass nur Berechtigte Zugriff auf die entsprechenden Unternehmensdaten haben. Das Risiko eines Datenlecks oder das Risiko der Verfälschung der Daten wächst.
Lösung	Sofern Berechtigungsnamen zum Beispiel intern definierten Nomenklaturen entsprechen sowie beschreibende Attribute wie Kategorie und Typ existieren, kann ein Nachweis generiert werden, dass ein übergreifendes Zugriffsrechte-Konzept durchgehend umgesetzt wird. Ebenso lassen sich Muster in den Berechtigungsstrukturen nachweisen und kontrollieren sowie eventuelle Abweichungen dokumentieren.

Garancy AIM kann Nachweis der Behebung liefern

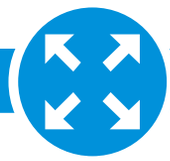
1.6 Rezertifizierung – fehlendes Rollenmodell

Einordnung

Problem	Eine qualifizierte Rezertifizierung ist nicht möglich, da kein wirksames Rollenmodell für Berechtigungen vorliegt und damit die Zahl an individuellen Berechtigungen sehr umfangreich ist. Nach der MaRisk AT 4.3.1 Tz. 2 und AT 7.2 Tz. 2 darf jeder Mitarbeiter nur über die Rechte verfügen, die er für seine Tätigkeit benötigt und diese sind nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) zu vergeben. Die Zusammenfassung von Berechtigungen in einem Rollenmodell ist möglich.
Risiko	Die Rezertifizierung von Berechtigungen soll sicherstellen, dass lediglich aktive und berechtigte Zugänge vorhanden sind. Dies dient dem Schutz der Unternehmensdaten. Ein Rollenmodell bietet hierbei Möglichkeiten zur Bündelung und kann daher Grundlage sein, die Datenmenge für den Rezertifizierungsprozess handhabbar zu machen.
Lösung	Es kann ein Nachweis generiert werden, welche Berechtigungen Mitarbeitern direkt bzw. über Rollen zugeordnet sind. Garancy AIM kann hierbei de facto auch zum Role Mining verwendet werden und auch auf diese Weise bei der Behebung der Feststellung unterstützen.

Garancy AIM kann Nachweis der Behebung liefern

1.7 Funktionstrennung – für Rollen nicht vorhanden



Einordnung

Problem	Eine angemessene Funktionstrennung der zur Weiterentwicklung und zum Betrieb einer Anwendung erforderlichen Rollen ist nicht vorhanden (z. B. haben Administratoren über das notwendige Maß hinausgehende Berechtigungen wie Erfassung/Änderung und Freigabe von Zahlungen). Nach der MaRisk AT 4.3.1 Tz. 1 und BTO Tz. 9 ist sicherzustellen, dass unvereinbare Tätigkeiten durch unterschiedliche Mitarbeiter durchgeführt werden. Durch entsprechende Verfahren und Schutzmaßnahmen ist sicherzustellen, dass bei IT-unterstützter Bearbeitung die Funktionstrennung eingehalten wird. Nach der BAIT 24 ist bei der Vergabe von Berechtigungen an Benutzer die Funktionstrennung sicherzustellen.
Risiko	Die Funktionstrennung dient dem Schutz des Unternehmens gegen Manipulationen. Es soll verhindert werden, dass Einzelpersonen weitreichende Entscheidungen treffen und umsetzen können. Bei fehlender Trennung zwischen Weiterentwicklung und Betrieb könnte beispielsweise absichtsweise eine Sicherheitslücke eingebaut werden, die schadhafte Buchungen zugunsten des Angreifers erlaubt.
Lösung	Soweit die relevanten Informationen über die CSV-Schnittstelle in das System geladen werden, kann ein Nachweis über alle im System vorhandenen Regeln und möglichen Verletzungen generiert werden. Bei der initialen Einführung von Regeln zur Funktionstrennung kann Garancy AIM in Form einer Ad-hoc-Analyse unterstützen.

Garancy AIM kann Nachweis der Behebung liefern

1.8 Vertreterfunktion – unkontrollierte Berechtigungsfreigabe

Einordnung

Problem	Ein Mitarbeiter in Vertreterfunktion kann sich selber seine beantragten Berechtigungen freigeben, da keine zusätzliche Prüfung bei der Freigabe von beantragten Rollen existiert. Nach der MaRisk AT 4.3.1 Tz. 1 müssen miteinander unvereinbare Tätigkeiten durch unterschiedliche Mitarbeiter durchgeführt werden.
Risiko	Ein solcher Vorgang verletzt die notwendige Funktionstrennung. Ohne diese Trennung können Einzelpersonen weitrechende Entscheidungen treffen, die unter anderem zur Manipulation oder zur Veruntreuung von Unternehmensdaten führen können.
Lösung	Die Behebung der Feststellung muss über eine Änderung des Prozesses realisiert werden. Ein Nachweis, dass ein derartiger Fall nicht eingetreten ist, kann in einer zukünftigen Version von Garancy AIM über die Time-Traveler-Funktion ausgewertet werden.

Garancy AIM kann Nachweis der Behebung liefern

1.9 Berechtigungsvergabe – keine Eskalationsstufen

Einordnung

Problem	Es sind keine Eskalationsstufen beim Antragsverfahren definiert. Eine zeitnahe Bearbeitung von Anträgen kann damit nicht sichergestellt werden. Nach BAIT 50 sind Eskalationsmechanismen in Prozessen zu etablieren.
Risiko	Ein in einem zeitlich angemessenen Rahmen funktionierendes Antragssystem ist notwendig, um eine Beeinträchtigung des Tagesgeschäftes zu verhindern. Diese Beeinträchtigungen können zur Unterhöhlung oder Umgehung des formalen Prozesses führen. Ein funktionierendes Berechtigungsmanagement kann so nicht mehr sichergestellt werden.
Lösung	Bei dieser Feststellung kann Garancy AIM in einer zukünftigen Version den Nachweis der Behebung der Feststellung erbringen. Es kann dann überprüft werden, wie schnell Prozesse durchlaufen werden, zum Beispiel mit der Darstellung der Zeiten, wann und von wem Genehmigungen erteilt wurden. Diese Funktionalität ist in der aktuellen Roadmap eingeplant.

Garancy AIM kann Nachweis der Behebung liefern

1.10 Berechtigungsvergabe – fehlende zweite Genehmigung

Einordnung

Problem	Die Neuanlage oder Änderung von Benutzern erfolgt ohne eine dokumentierte Genehmigung einer zweiten, hierzu berechtigten Person. Nach BAIT 26 ist durch Genehmigungs- und Kontrollprozesse bei der Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen für Benutzer sicherzustellen, dass die Vorgaben des Berechtigungskonzepts eingehalten werden.
Risiko	Durch die fehlende Kontrolle und Dokumentation bei der Berechtigungsvergabe existieren keine Hindernisse oder im Zweifelsfall Nachweise für die Manipulation oder Veruntreuung von Unternehmensdaten.
Lösung	Bei dieser Feststellung kann Garancy AIM in einer zukünftigen Version den Nachweis der Behebung der Feststellung erbringen. Es kann dann ausgewertet werden, dass durchgehend ein vom Erstgenehmiger unterschiedlicher Zweitgenehmiger vorhanden war. Diese Funktionalität ist in der aktuellen Roadmap eingeplant.

Garancy AIM kann Nachweis der Behebung liefern

1.11 Mitarbeiterversetzung – fehlende Genehmigung für alte Berechtigungen

Einordnung

Problem	Bei Wechsel eines Mitarbeiters innerhalb des Unternehmens kann dieser neben den neuen Berechtigungen vorübergehend alle oder einen Teil seiner früheren Berechtigungen behalten, sofern sein neuer Vorgesetzter dies erlaubt. Die Genehmigung des früheren Vorgesetzten wird nicht eingeholt. Nach der MaRisk AT 4.3.1 Tz. 1, AT 4.3.1 Tz. 2 und BTO Tz. 9 sind Berechtigungen und Kompetenzen nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) zu vergeben und bei Bedarf zeitnah anzupassen. Bei Arbeitsplatzwechsel sind Interessenkonflikte zu vermeiden. Die Funktionstrennung ist durch entsprechende Verfahren und Schutzmaßnahmen sicherzustellen.
Risiko	Ohne die Beteiligung aller involvierten Vorgesetzten kann nicht sichergestellt werden, dass nur notwendige Berechtigungen vergeben sind. Eine Überberechtigung erhöht das Risiko, dass die Vertraulichkeit oder die Integrität von Unternehmensdaten verletzt wird.
Lösung	Bei dieser Feststellung kann Garancy AIM in einer zukünftigen Version den Nachweis der Behebung erbringen. Sobald der Kern der Feststellung durch Änderungen in der Workflow Engine behoben ist, kann mittels Garancy AIM überprüft werden, wie schnell Prozesse durchlaufen, zum Beispiel mit der Darstellung der Zeiten, wann die Genehmigung früherer und aktueller Vorgesetzten erteilt wurde. Diese Funktionalität ist in der aktuellen Roadmap eingeplant.

Garancy AIM kann Nachweis der Behebung liefern (zukünftig)

1.12 Mitarbeiterversetzung – fehlende Cool-Down-Phase

Einordnung

Problem	Bei Wechsel eines Mitarbeiters innerhalb des Unternehmens wird eine gegebenenfalls notwendige Cool-Down-Phase für Berechtigungen nicht umgesetzt (wechselt zum Beispiel ein Mitarbeiter aus dem Markt-Bereich in den Marktfolge-Bereich, so muss zwischen Entzug der Markt-Berechtigungen und Zuweisung der Marktfolge-Berechtigungen eine bestimmte Zeitdauer liegen). Nach der MaRisk AT 4.3.1 Tz. 2 und BTO Tz. 9 sind bei Wechsel von Mitarbeitern der Handels- und Markt-Bereiche in nachgelagerte Bereiche und Kontrollbereiche angemessene Übergangsfristen vorzusehen. Bei Arbeitsplatzwechsel sind Interessenkonflikte zu vermeiden. Die Funktionstrennung ist durch entsprechende Verfahren und Schutzmaßnahmen sicherzustellen.
Risiko	Eine fehlende Cool-Down-Phase kann zur Überberechtigung oder zur Verletzung der Funktionstrennung führen. In beiden Fällen erhöht sich das Risiko, dass Unternehmensdaten nicht vertraulich behandelt oder manipuliert werden.
Lösung	Bei dieser Feststellung kann Garancy AIM den Nachweis der Behebung direkt durch die Time-Traveler-Funktion erbringen. Dabei könnte nachgewiesen werden, dass bei Mitarbeitern, bei denen eine Cool-Down-Phase notwendig ist, alte Berechtigungen bereits entzogen werden, während die Zuweisung neuer Berechtigungen durch den Prozess temporär verhindert wird. Darüber hinaus ist in der aktuellen Roadmap eingeplant, einzelne Prozessschritte auswerten zu können.

Garancy AIM kann Nachweis der Behebung liefern (zukünftig)

1.13 Berechtigungsvergabe – vorhandene Überberechtigungen

Einordnung

Problem	Es existieren Überberechtigungen, da Berechtigungen nicht nach dem Need-to-know-Prinzip vergeben werden oder eine Rezertifizierung nicht oder nicht sachgerecht durchgeführt wird. Nach der MaRisk AT 4.3.1 Tz. 2 müssen Berechtigungen und Kompetenzen nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) vergeben werden und sind bei Bedarf zeitnah anzupassen. Nach der BAIT 24 ist bei der Vergabe von Berechtigungen der Sparsamkeitsgrundsatz (Need-to-know-Prinzip) sicherzustellen.
Risiko	Eine Überberechtigung erhöht das Risiko, dass Unternehmensdaten manipuliert oder nicht vertraulich behandelt werden.
Lösung	Bei dieser Feststellung kann Garancy AIM zum Teil verwendet werden, um den Nachweis der Behebung der Feststellung zu erbringen. Zum einen kann mittels einer Ausreißeranalyse überprüft werden, ob Mitarbeiter zum Beispiel innerhalb eines Bereiches/einer Kostenstelle/einer Organisationseinheit Überberechtigungen besitzen. In einer zukünftigen Garancy-AIM-Version werden auch die Informationen aus der Rezertifizierung bereitstehen, sodass auch der Nachweis einer Rezertifizierung erbracht werden kann.

Garancy AIM kann Nachweis der Behebung liefern (zukünftig)

1.14 Berechtigungsvergabe – keine Übersicht über genehmigte Zugriffsrechte

Einordnung

Problem	Es existiert keine zuverlässige zentrale Datenbank für genehmigte Zugriffsrechte. Nach der BAIT 28 ist die Einrichtung, Änderung, Deaktivierung und Löschung von Berechtigungen und die Rezertifizierung nachvollziehbar und auswertbar zu dokumentieren.
Risiko	Eine mangelnde Dokumentation im Zugriffsrechtemanagement kann zu Überberechtigungen führen oder die Funktionstrennung gefährden. Auch kann im Zweifelsfall der Nachweis eines Zugangs erschwert bzw. unmöglich sein.
Lösung	Bei dieser Feststellung kann Garancy AIM einen Nachweis einer Behebung erbringen. Es kann überprüft werden, wer die jeweiligen Rechte über die Workflow-Komponente zur Berechtigungsbeantragung genehmigt hat. Diese Funktionalität ist in der aktuellen Roadmap eingeplant und wird zukünftig zur Verfügung stehen. Aktuell kann je nach Konfiguration des Workflows überprüft werden, dass eine Genehmigung erfolgt ist, jedoch nicht wann oder durch wen.

Garancy AIM kann Nachweis der Behebung liefern (zukünftig)

1.15 Berechtigungsvergabe – kein Vier-Augen-Prinzip

Einordnung

Problem	Im Genehmigungsverfahren bei der Beantragung von Berechtigungen kommt es vor, dass eine mehrstufige Genehmigung von ein und derselben Person ausgeübt wird und somit ein Vier-Augen-Prinzip nicht vollumfänglich sichergestellt wird. Nach der BAIT 26 sind bei dem Verfahren zur Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen die Vorgaben des Berechtigungskonzepts durch Genehmigungs- und Kontrollprozesse sicherzustellen.
Risiko	In einem solchen Fall ist die Funktionstrennung nicht sichergestellt. Die Funktionstrennung soll sicherstellen, dass keine weitreichenden Entscheidungen von Einzelpersonen getroffen werden können, um das Unternehmen vor Missbrauch und/oder Manipulation zu schützen.
Lösung	Die Behebung der Feststellung muss über eine Änderung des Prozesses realisiert werden. Ein Nachweis, ob die Prozesse angepasst wurden, kann in einer zukünftigen Version von Garancy AIM über die Time-Traveler-Funktion erstellt werden. Grundlage dafür ist die Auswertungsmöglichkeit der Genehmigungen.

Garancy AIM kann Nachweis der Behebung liefern (zukünftig)

1.16 Funktionstrennung – keine Unterstützung für Infrastrukturkomponenten

Einordnung

Problem	Die Infrastrukturkomponenten einer Anwendung (Betriebssystem, Datenbank, Anwendung) können von derselben Person administriert werden. Nach BAIT 24 sind bei der Vergabe von Berechtigungen an Benutzer Interessenskonflikte des Personals zu vermeiden.
Risiko	Es besteht das Risiko einer Manipulation der Daten oder der Konfiguration der Anwendung, wodurch die Integrität, die Authentizität und die Vertraulichkeit der Daten nicht sichergestellt sind.
Lösung	Die Behebung der Feststellung setzt voraus, dass die Berechtigungen durch ein Attribut jeweils sowohl einer Komponente als auch einer Anwendung zuzuordnen sind sowie anhand eines Attributs erkannt werden kann, ob es sich um Administrator-Berechtigungen handelt. Ist dies der Fall, so kann ein entsprechender Nachweis über Garancy AIM erstellt werden, ob es User gibt, die administrativen Zugriff auf mehrere Komponenten einer Anwendung besitzen.

Garancy AIM kann Nachweis der Behebung liefern (zukünftig)

1.17 Funktionstrennung – Regelverstöße innerhalb von Business-Rollen

Einordnung

Problem	Es ist möglich, Business-Rollen zu beantragen, die zu Funktionstrennungs-verstößen führen, ohne dass dafür ein gesonderter Workflow zur expliziten Risikoakzeptanz gestartet wird. Nach der BAIT 24 ist bei der Vergabe von Berechtigungen an Benutzer die Funktionstrennung sicherzustellen.
Risiko	Die Sicherstellung der Funktionstrennung soll das Unternehmen vor Missbrauch oder Manipulation schützen.
Lösung	Die Behebung der Feststellung muss über eine Änderung des Prozesses realisiert werden. Ein Nachweis, ob ein derartiger Fall eingetreten ist, kann in einer zukünftigen Version von Garancy AIM über die Prüfung der Prozessbeteiligten durchgeführt werden. Sollte ein Funktionstrennungsverstoß generiert worden sein, so muss im Workflow ein zusätzlicher Genehmiger erkennbar sein.

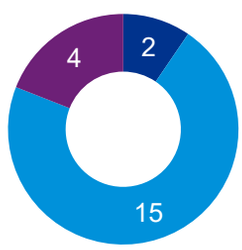
Garancy AIM kann Nachweis der Behebung liefern (zukünftig)

Fazit

Der Garancy AIM kann ein Unternehmen dabei unterstützen, die Aufgaben der Funktionstrennung, der Rezertifizierung und der minimalen Berechtigungsvergabe zu lösen. Diese Prinzipien sollen direkt das geistige Eigentum des Unternehmens vor Veruntreuung oder Manipulation schützen.

Neben der direkten Überwachung von Berechtigungen können auch historische Reports erstellt werden, die eine Weiterentwicklung des Berechtigungsmanagements erlauben sowie die Ergebnisse von bereits gelaufenen Prozessen auswerten zu können. Außerdem lassen sich Kennwerte (z. B. mittlere Bearbeitungsdauer) für Prozesse in Verbindung mit dem Berechtigungsmanagement nutzerfreundlich ermitteln. Diese Kennwerte können genutzt werden, um den Nachweis erbringen, dass eine betrachtete Feststellung gelöst wurde oder um zu erkennen, dass sie noch zu lösen ist.

Direkte Änderungen im Vergabe-, Änderungs- oder Entzugsprozess von Berechtigungen können nicht vorgenommen werden. Die Effekte solcher Änderungen lassen sich allerdings nachweisen. KPMG kann mit dem jeweiligen Unternehmen die problematischen Prozesse analysieren und technische wie auch manuelle Lösungen erarbeiten.



kann durch Garancy AIM behoben werden

Garancy AIM kann Nachweis der Behebung liefern

kann durch KPMG-Dienstleistung behoben werden

2. Identifikation und Authentifizierung

2.1 Externe Mitarbeiter – unvollständiger Überblick

Einordnung

Problem	Überblick über externe Mitarbeiter und deren Zugriffe auf Unternehmensdaten ist nur unvollständig vorhanden. Nach der BAIT 28 ist die Einrichtung, Änderung, Deaktivierung und Löschung von Berechtigungen und die Rezertifizierung nachvollziehbar und auswertbar zu dokumentieren.
Risiko	Die Integrität und Vertraulichkeit von Daten und geistigem Eigentum des Unternehmens kann ohne einen vollständigen Überblick über die Zugangsberechtigungen von externen Mitarbeitern nicht sichergestellt werden.
Lösung	Im IAM-System können externe Mitarbeiter (z. B. anhand der Nomenklatur ihrer Benutzerkennung oder über händisch gepflegte Attribute) als solche gekennzeichnet werden. Sofern dies geschehen ist, kann mit Garancy AIM die Feststellung direkt behoben werden. Es kann eine Auswertung erstellt werden, welche Berechtigungen externe Mitarbeiter besitzen.

Kann durch Garancy AIM behoben werden

2.2 Technische Benutzer – keine Zuordnung

Einordnung

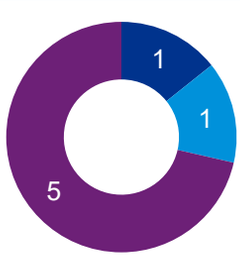
Problem	Nicht zu allen technischen Benutzern liegt eine Zuordnung zu einem verantwortlichen Mitarbeiter vor. Nach der BAIT 25 müssen nicht personalisierte Berechtigungen jederzeit zweifelsfrei einer handelnden Person zuzuordnen sein. In begründeten Ausnahmefällen sind Abweichungen zu dokumentieren und die daraus resultierenden Risiken sind zu genehmigen und zu dokumentieren.
Risiko	Technischen Benutzern sollte eine eindeutige Verantwortlichkeit zugewiesen werden, um Missbrauch oder falsche Verwendung der gewährten Zugriffe vorzubeugen. Ein solcher Missbrauch gefährdet die Verfügbarkeit, die Integrität und die Vertraulichkeit der zugänglichen Unternehmensdaten.
Lösung	Bei dieser Feststellung kann Garancy AIM je nach Art der Behebung einen Nachweis der Umsetzung erbringen. Können im IAM (z. B. durch Nomenklatur, bestimmte HR-Attribute oder händische Pflege) technische Benutzer eindeutig erkannt werden, kann über Garancy AIM eine Auswertung erzeugt werden, ob das Zuordnungsattribut durchgehend gefüllt ist und sich durchgehend nur auf aktive Benutzer bezieht.

Garancy AIM kann Nachweis der Behebung liefern

Fazit

Der Garancy AIM erlaubt die Pflege und Überwachung von Berechtigungen aller Art. So ist es möglich, die Berechtigungen von internen und externen Mitarbeitern jederzeit abzurufen. Auch Attribute von technischen Benutzern, wie beispielsweise die Zuordnung, können eingesehen und auf Lücken überprüft werden. Lücken in der Zuordnung von Attributen oder unpassende Berechtigungen gefährden die Integrität, die Vertraulichkeit und erlauben die Manipulation von Unternehmensdaten und geistigem Eigentum.

Eine Überwachung der mit Accounts durchgeführten Aktionen kann nicht vorgenommen werden. KPMG kann mit dem jeweiligen Unternehmen passende Prozesse erarbeiten und ggf. bei der Auswahl geeigneter Tools unterstützen.



kann durch Garancy AIM behoben werden

Garancy AIM kann Nachweis der Behebung liefern

kann durch KPMG-Dienstleistung behoben werden

3. Monitoring

3.1 Berechtigungsauswertung – kein Überblick über angebundene Systeme

Einordnung

Problem	Es kann kein Überblick über die bereits angebundenen Systeme an das IAM-Tool gegeben werden. Nach MaRisk AT 12 4.1 muss ein vollständiger und aktueller Überblick über die Methoden und Verfahren existieren, die zur Risikoquantifizierung verwendet werden. Da die Anbindung an ein IAM-Tool Auswirkungen auf die Risikobetrachtung besitzt, muss somit eine Übersicht der angebundenen Systeme existieren.
Risiko	Soweit keine vollständige und aktuelle Einschätzung der Risiken existiert, kann kein vernünftiger risikobasierter Ansatz beim Berechtigungsmanagement gefahren werden. Ein optimaler und budgeteffizienter Schutz der Geschäftsprozesse und der dafür notwendigen IT-Systeme kann somit nicht gewährleistet werden.
Lösung	Mit Garancy AIM kann eine Auswertung erstellt werden, welche Systeme an das IAM-Tool angebunden sind.

Kann durch Garancy AIM behoben werden

3.2 Berechtigungsauswertung – keine historischen Reports

Einordnung

Problem	Es können keine zeitraumbezogenen oder historischen Reports erstellt werden. Nach der BAIT 28 ist die Einrichtung, Änderung, Deaktivierung und Löschung von Berechtigungen und die Rezertifizierung nachvollziehbar und auswertbar zu dokumentieren.
Risiko	Diese Reports dienen neben der Beobachtung der Entwicklung des Berechtigungsmanagements auch dem Nachweis gegenüber regulatorischen Anforderungen. Eine Nichterfüllung dieser Anforderungen kann erhebliche wirtschaftliche Folgen haben. Außerdem ist auch eine unternehmensinterne Beweisführung bzw. Nachvollziehbarkeit nach einem Zwischenfall erschwert oder nicht möglich.
Lösung	Mit Garancy AIM können sowohl zeitraumbezogene als auch historische Reports erstellt werden. Garancy AIM bietet mit der Time-Traveler-Funktion verschiedene Perspektiven auf die Berechtigungsstruktur sowie eine Statushistorie (Welche Berechtigungen hatte ein Mitarbeiter in einem bestimmten Zeitraum?) oder eine Änderungshistorie (Welche Berechtigungen haben sich in einem bestimmten Zeitraum geändert?).

Kann durch Garancy AIM behoben werden

3.3 Fehlende Rechteprüfung in Zielsystemen/Anwendungen

Einordnung

Problem	Die Rezertifizierung von Anwendungen basiert nicht auf den tatsächlich genehmigten und implementierten Einzelzugriffsrechten (Soll-Ist-Vergleich). Nach der BAIT 29 wird festgehalten, dass überprüfbar gemacht werden soll, dass die Berechtigungen nur wie vorgesehen eingesetzt werden. Außerdem greift hier als Anforderung die BAIT 26, die implizit vorsieht, dass sichergestellt wird, dass die Antragslage/der Soll-Zustand dem Ist-Zustand entspricht.
Risiko	Eine mangelhafte oder auf falschen Daten basierende Rezertifizierung erhöht das Risiko unberechtigter Zugriffe. Je nach Anwendung können Unternehmensdaten oder geistiges Eigentum verbreitet, manipuliert oder unzugänglich gemacht werden.
Lösung	Die Zusammensetzung von Berechtigungen bis auf die Transaktionsebene kann via CSV in Garancy AIM geladen werden. Somit können über Garancy-AIM-Reports bis auf Transaktionsebene erstellt werden, die sich als Grundlage einer derartigen Rezertifizierung eignen.

Kann durch Garancy AIM behoben werden

3.4 Einzelrechte – keine Überprüfung

Einordnung

Problem	Die Zusammensetzung von Berechtigungsgruppen aus Einzelrechten wird nur unzureichend überprüft. Die BAIT23 fordert, dass Berechtigungen so ausgestaltet sind, wie es den organisatorischen und fachlichen Vorgaben des Instituts entspricht. Dies bedeutet, dass ein Prüfprozess zum Beispiel in Form der Rezertifizierung existieren sollte, der regelmäßig oder anlassbezogen die Zusammensetzung der Berechtigungsgruppen auf die weiter bestehende fachliche Notwendigkeit sämtlicher enthaltener Einzelrechte prüft.
Risiko	Die mangelnde Prüfung und Sicherstellung der Berechtigungs-zusammensetzungen erhöht das Risiko der Überberechtigung. Eine solche Überberechtigung gefährdet die Vertraulichkeit und die Integrität der freigegebenen Systeme, Anwendungen und Daten.
Lösung	Die Zusammensetzung von Berechtigungen bis hin auf Transaktionsebene kann via CSV in Garancy AIM geladen werden. Somit können über Garancy-AIM-Reports bis auf Transaktionsebene erstellt und ausgewertet werden. Im Rahmen der Rollenrezertifizierung liefert Garancy AIM die Informationen über die Einzelrechte in Form einer Hierarchiedarstellung der jeweils zu rezertifizierenden Rolle.

Kann durch Garancy AIM behoben werden

3.5 Funktionstrennung – kein Verfahren für Regelverstöße

Einordnung

Problem	Es gibt kein dokumentiertes Verfahren, wie die vom IAM-System erkannten Verstöße gegen die Funktionstrennung behandelt und die betreffenden Konflikte gelöst werden. Nach BAIT 28 sind die Einrichtung, Änderung, Deaktivierung und die Rezertifizierung nachvollziehbar und auswertbar zu dokumentieren. Zur Rezertifizierung gehört indirekt auch die Legitimierung oder Auflösung von Funktionstrennungsverstößen. Um Funktionstrennungsverstöße zu vermeiden, wird nach AT 4.3.1 Tz. 1 zudem geregelt, dass beim Wechsel von Mitarbeitern der Handels- und Marktbereiche in nachgelagerte Bereiche und Kontrollbereiche angemessene Übergangsfristen vorzusehen sind („Cooling-Off“), die nicht gegen das Verbot der Selbstprüfung und -überprüfung verstoßen.
Risiko	Eine unzureichende Umsetzung der Funktionstrennung, auch im Hinblick auf den Umgang mit Verstößen, birgt das Risiko, dass Einzelpersonen weitreichende Befugnisse erlangen, die eine Veruntreuung oder Manipulation von unternehmenskritischen Daten und Anwendungen erlauben.
Lösung	Die Behebung der Feststellung muss über eine Änderung des Prozesses realisiert werden. Ein Nachweis, wie lange es durchschnittlich oder konkret dauert, um Funktionstrennungsverstöße zu beheben, kann von Garancy AIM über die Time-Traveler-Funktion erstellt werden. Daraus kann auch abgelesen werden, wie die Behebung umgesetzt wurde (z. B. Berechtigungsentzug, Sondergenehmigung, Umklassifizierung).

Garancy AIM kann Nachweis der Behebung liefern

3.6 Rezertifizierung – nicht definierte Zeitabstände

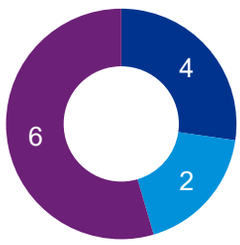
Einordnung

Problem	Die Zeitabstände der Rezertifizierung sind nicht für alle Anwendungen definiert. Nach MaRisk AT 4.3.1 Tz. 2 sind IT-Berechtigungen, Zeichnungsberechtigungen sowie sonstige eingeräumte Kompetenzen innerhalb angemessener Fristen regelmäßig und anlassbezogen zu rezertifizieren. Die Fristen orientieren sich dabei an der Bedeutung der Prozesse und, bei IT-Berechtigungen, dem Schutzbedarf verarbeiteter Informationen.
Risiko	Eine regelmäßige Rezertifizierung aller Anwendungen entsprechend ihrer Kritikalität ist notwendig, um Überberechtigungen zu verhindern. Die Rezertifizierung dient damit direkt dem Schutz der unternehmenseigenen Daten hinsichtlich Vertraulichkeit und Integrität.
Lösung	Bei dieser Feststellung kann Garancy AIM in einer zukünftigen Version teilweise unterstützen, indem ein Nachweis geliefert werden kann, in welchem Zeitraum welche Anwendungen/User rezertifiziert worden sind. Dabei kann festgestellt werden, welche Anwendungen noch gar nicht rezertifiziert worden sind bzw. wo es auch noch keine definierten Zeitabstände gibt.

Garancy AIM kann Nachweis der Behebung liefern

Fazit

Der Garancy AIM erlaubt einen tiefen Einblick in die Zusammensetzungen verschiedenster Berechtigungen. Somit ist es möglich, alle grundlegenden Prinzipien der Berechtigungsvergabe im Hinblick auf fachliche Notwendigkeit und Funktionstrennung zu überwachen. Diese Überwachung ist auch auf die Vergangenheit in Form von historischen Reports ausdehnbar. Auch Kennzahlen, wie eine durchschnittliche Prozessdauer bzw. der Prozessablauf, lassen sich auswerten und entsprechend optimieren.



Eine mangelnde Kontrolle kann zur Missachtung der beschriebenen Regeln, Anforderungen und Prinzipien führen, welche zum Schutz des Unternehmens vor Manipulation, Veruntreuung oder Sabotage dienen.

Notwendige Prozessanpassungen, insbesondere im Rahmen der Rezertifizierung, lassen sich mit Garancy AIM nicht umsetzen oder nachweisen. Hierzu ist zum Beispiel eine Anpassung im verwendeten Workflow-Tool notwendig, sodass auch an dieser Stelle der Nachweis geführt werden muss. KPMG kann bei der Anpassung der Prozesse unterstützen.

- kann durch Garancy AIM behoben werden
- Garancy AIM kann Nachweis der Behebung liefern
- kann durch KPMG-Dienstleistung behoben werden

4. Superuser

4.1 Berechtigungsauswertung – nicht erkennbare kritische Berechtigungen

Einordnung

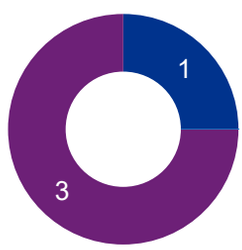
Problem	Kritische Berechtigungen sind nicht erkennbar. Nach BAIT 24 wird gefordert, dass Berechtigungskonzepte den Umfang und die Nutzungsbedingungen der Berechtigungen für die IT-Systeme konsistent zum ermittelten Schutzbedarf sowie vollständig und nachvollziehbar ableitbar für alle von einem IT-System bereitgestellten Berechtigungen festlegen.
Risiko	Benutzer mit kritischen Berechtigungen können innerhalb eines Unternehmens weitreichende Befugnisse erlangen, wenn sie nicht ausreichend kontrolliert werden. Es besteht das Risiko, dass Einzelpersonen unternehmenskritische Daten oder geistiges Eigentum manipulieren, veruntreuen und/oder vernichten können.
Lösung	Diese Feststellung kann mit Garancy AIM direkt behoben werden, sobald im IDM eine Risikobewertung der einzelnen Rollen, Gruppen und Ressourcen vorgenommen wurde. Dazu bietet die Garancy IAM Suite ein durchgehendes Risikomodell.

Kann durch Garancy AIM behoben werden

Fazit

Der Garancy AIM erlaubt es, als kritisch markierte Berechtigungen, wie beispielsweise die eines Superusers, zu überwachen. Diese Kontrolle ist notwendig, damit Einzelpersonen nicht die Befugnisse erlangen können, unternehmenskritische Prozesse durch Manipulation, Verbreitung oder Vernichtung von Daten zu stören. Zudem sollten in den Auswertungsreports immer kritische Berechtigungen erkennbar sein.

Notwendige Anpassungen an Prozessen oder Governance lassen sich mit Garancy AIM nicht umsetzen oder nachweisen. KPMG kann bei der Anpassung der Prozesse bzw. der Governance unterstützen.



kann durch Garancy AIM behoben werden

Garancy AIM kann Nachweis der Behebung liefern

kann durch KPMG-Dienstleistung behoben werden

5. Vorgaben zur Berechtigungsmodellierung

5.1 Funktionstrennung – erstellbare Business-Rollen mit Regelverstößen

Einordnung

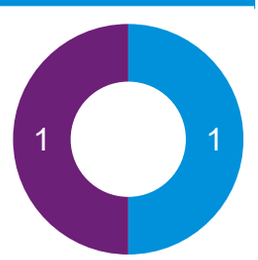
Problem	Funktionstrennung wird nicht bei der Erstellung von Berechtigungsrollen angewendet (d. h. es ist möglich, Business-Rollen zu erstellen, die aus Funktionstrennungssicht konfliktäre Gruppen beinhalten). Nach BAIT 24 soll sichergestellt werden, dass Berechtigungskonzepte die Vergabe von Berechtigungen an Benutzer nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) vergeben, um die Funktionstrennung zu wahren und Interessenkonflikte des Personals zu vermeiden.
Risiko	Die Missachtung der Funktionstrennung erhöht das Risiko, einen Nutzer mit Berechtigungen auszustatten, die einen unternehmenskritischen Einfluss ermöglichen. Beispielsweise könnten Unternehmensdaten von Einzelpersonen manipuliert, gelöscht oder verbreitet werden.
Lösung	Bei dieser Feststellung kann Garancy AIM in einer zukünftigen Version den Nachweis der Behebung der Feststellung erbringen. Dazu muss dem Garancy AIM das Regelwerk in einer Form bekannt gemacht werden, die das Garancy AIM auswerten kann. Die Auswertung kann komplex werden, wenn es verschiedene Möglichkeiten gibt, Funktionstrennungskonflikte zu erzeugen (zum Beispiel jeweils gemischt über Anwendungsbezeichnungen, Abteilungen, MaRisk-Kennzeichen, Standorte).

Garancy AIM kann Nachweis der Behebung liefern (zukünftig)

Fazit

Mit dem Garancy AIM ist es möglich, das Thema Konflikte in Bezug auf die Funktionstrennung auszuwerten. Dabei müssen allerdings im Vorfeld die entsprechenden Berechtigungen, zum Beispiel mit den jeweiligen Kennzeichen, nach einer vordefinierten Funktionstrennungs-Matrix Garancy-AIM-tauglich gekennzeichnet werden. Auch beim Thema Berechtigungsrollen muss ein Unternehmen im Vorfeld Modellierarbeit leisten, damit die Berechtigungen ordentlich im IDM-System hinterlegt und mit dem Garancy AIM auswertbar sind. KPMG hat bereits viele Kunden und Projekte beim Aufbau eines ganzheitlichen Berechtigungsmanagementkonzeptes unterstützt und kann je nach Ausgangslage als Kooperationspartner von Beta Systems die notwendigen Vorarbeiten begleiten.

Notwendige Anpassungen an Prozessen oder Governance lassen sich mit Garancy AIM nicht umsetzen oder nachweisen. KPMG kann bei der Anpassung der Prozesse bzw. der Governance unterstützen.



kann durch Garancy AIM behoben werden

Garancy AIM kann Nachweis der Behebung liefern

kann durch KPMG-Dienstleistung behoben werden

6. Berechtigungskonzepte

6.1 Berechtigungskonzept – fehlt, unvollständig, veraltet

Einordnung

Problem	Für die Weiterentwicklung und für den Betrieb von Anwendungen fehlen, sind unvollständig oder nicht aktuell: — Fachvorgaben — Dokumentationen des Sollzustands (fachliches und technisches Design) — Berechtigungskonzept — angemessene Testkonzepte — Definitionen von Testobjekten — ein Testfallportfolio — ein Betriebshandbuch Nach BAIT 24 soll über Berechtigungskonzepte sichergestellt werden, dass die Vergabe von Berechtigungen an Benutzer nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) geschieht, die Funktionstrennung gewahrt wird und Interessenkonflikte des Personals vermieden werden.
Risiko	Ohne Dokumentation des Sollzustands und der Prozesse in Verbindung mit der Anwendung besteht das Risiko der Missachtung der Funktionstrennung, der Administrationswege und der Zuordnung von fachlich unpassenden Berechtigungen an Benutzer. Damit erhöht sich das Risiko, dass ein Nutzer mit Berechtigungen ausgestattet wird, die unternehmenskritischen Einfluss ermöglichen. Beispielsweise könnten Unternehmensdaten von Einzelpersonen manipuliert, gelöscht oder verbreitet werden. Nicht oder nur mangelhaft durchgeführte Tests können zum einen aufgrund nicht erkannter Fehler im Betrieb zu Ausfällen führen. Zum anderen besteht das Risiko, dass durch eingebaute schadhafte Funktionalitäten von Entwicklern oder Dritten die Integrität und Vertraulichkeit der Daten gefährdet wird.
Lösung	Bei dieser Feststellung kann ein Teil der Nachweise, dass die Feststellung behoben wurde, über Garancy AIM erbracht werden. Sofern die Dokumentation der Berechtigungen über das IAM-System oder in den Zielsystemen direkt umgesetzt wird, kann eine Auswertung erzeugt werden, die eine KPI liefert, welche dokumentationspflichtigen Attribute in welchem Maße dokumentiert wurden.

Garancy AIM kann Nachweis der Behebung liefern

6.2 Berechtigungskonzept – keine Templates

Einordnung

Problem	Es existiert kein Template für Berechtigungskonzepte. Die Berechtigungskonzepte unterscheiden sich daher sehr stark, je nach Motivation und Wissen des Erstellers. Um das Prinzip der Berechtigungssteuerung und der zugehörigen Regelprozesse in den jeweiligen Systemen und Anwendungen verstehen und umsetzen zu können, ist die Erstellung eines Berechtigungskonzeptes für das entsprechende IT-System notwendig. Damit durchgehend alle relevanten Informationen für die Berechtigungssteuerung in verwertbarer Form vorliegen, ist ein Template notwendig, um größere Heterogenität zu vermeiden.
Risiko	Eine schlechte oder mangelnde Dokumentation von Berechtigungskonzepten erlaubt keine fundierte Entscheidung für die Berechtigungsvergabe. Das Risiko, dass falsche oder zu weitgehende Berechtigungen erteilt werden, wächst.
Lösung	Bei dieser Feststellung kann Garancy AIM in Teilen einen Nachweis einer Behebung der Feststellung liefern. Es kann beispielsweise nachgewiesen werden, dass alle Berechtigungen im IAM gleichartig dokumentiert sind und zum Beispiel Nomenklaturen für Berechtigungen eingehalten werden.

Garancy AIM kann Nachweis der Behebung liefern

6.3 Berechtigungskonzept – keine Nomenklatur

Einordnung

Problem	Es gibt keine zentrale Vorgabe für eine inhaltlich sprechende Nomenklatur für die jeweiligen Business-Rollen. Damit die von der BAIT geforderte Einrichtung passgenauer Berechtigungen inklusive regelmäßiger Überprüfungen (wie in BAIT 23 in Verbindung mit BAIT26 und 27 gefordert) eingehalten werden kann, muss für alle Beteiligten eindeutig erkennbar sein, welche Funktionalitäten den Berechtigungen (im Beispiel: den Business-Rollen) zugeordnet sind. Dieser Anforderung kann man sich unter anderem durch eine inhaltlich sprechende Nomenklatur annähern.
Risiko	Eine schlechte oder mangelnde Beschreibung von Berechtigungen erlaubt keine fundierte Entscheidung beim Beantragungsprozess sowie bei einer regelmäßigen Rezertifizierung. Das Risiko, dass falsche oder zu weitgehende Berechtigungen beantragt, beibehalten oder gelöscht werden, wächst.
Lösung	Es kann eine Übersicht generiert werden, in der aufgezeigt wird, ob und welchen Nomenklaturen/Kategorien die Business-Rollen entsprechen.

Garancy AIM kann Nachweis der Behebung liefern

6.4 Berechtigungen – unzureichende Beschreibungen

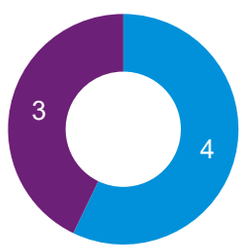
Problem	Beschreibungen von Berechtigungen sind nicht aussagekräftig genug, um eine qualifizierte Bewertung im Rahmen von Beantragungs- oder Rezertifizierungsprozessen zuzulassen. Dass eine Rezertifizierung stattfinden muss, wird von der MaRisk und der BAIT vorgegeben. Um die darin zu bewertenden Berechtigungen qualifizieren zu können, bedarf es einer eindeutig sprechenden Beschreibung der Berechtigungen, die für sämtliche an der Rezertifizierung beteiligten Akteure verständlich ist. Das gleiche gilt für die Beurteilung von Berechtigungen im Beantragungsprozess.
Risiko	Lücken im Beantragungs- oder Rezertifizierungsprozess können zu Überberechtigungen oder zum Umgehen des Prozesses, weil er nicht alltagstauglich ist, führen. Beide Fälle erhöhen signifikant das Risiko, dass Unternehmensdaten oder geistiges Eigentum von unberechtigten Einzelpersonen veruntreut, manipuliert oder veröffentlicht werden können.
Lösung	Bei dieser Feststellung kann Garancy AIM teilweise den Nachweis einer Behebung der Feststellung liefern. Es kann eine Übersicht erstellt werden, die beispielsweise auflistet, welche Gruppen keine Beschreibung besitzen oder deren Beschreibung bestimmten, nicht ausreichenden Kriterien entspricht (zum Beispiel Anlagedatum oder letztes Änderungsdatum). Ein vollständiger Nachweis der Umsetzung über solche Minimalziele hinweg wird nur durch systematisches persönliches Überprüfen der Beschreibungen möglich sein. Dazu könnten alle Beschreibungen gruppiert nach Typ, Kategorie oder anderen Attributen aufgelistet und verglichen werden.

Einordnung

Garancy AIM kann Nachweis der Behebung liefern

Fazit

In der Kategorie Berechtigungskonzepte und deren Inhalte kann der Garancy AIM in vielen Fällen Nachweise liefern, ob und in welcher Qualität die Inhalte von Berechtigungskonzepten, insbesondere bei der Beschreibung von Berechtigungen, vorliegen. Vorhergehend muss aber eine vollständige Berechtigungsmanagement-Governance aufgestellt, dokumentiert, qualitätsgesichert und gelebt werden. KPMG kann hier mit ihrer Expertise diesen Aufbau unterstützen.



kann durch Garancy AIM behoben werden

Garancy AIM kann Nachweis der Behebung liefern

kann durch KPMG-Dienstleistung behoben werden

Feststellungen, die durch KPMG-Dienstleistung behoben werden können

Bei Feststellungen, die keinen Bezug zu Garancy AIM haben, kann durch Dienstleistungen von KPMG unterstützt werden. Hierbei wird das Thema Identity & Access Management ganzheitlich betrachtet und es werden sowohl die fachlichen als auch die organisatorischen sowie die technischen Aspekte auf einen gemeinsamen Nenner gebracht, zum Beispiel:

— fachlich: Identifizierung fachlicher Anforderungen, Unterstützung bei der Abbildung von Funktionstrennungen und Business-Rollen

— technisch: Integration von IAM-Systemen in eine bestehende IT-Landschaft und anschließende Übergabe an den Betrieb; Orchestrierung von Authentifizierung, Antragsworkflows, Rule Engine, Rechteadministration, Provisionierung, Rezertifizierung

— organisatorisch: Definition und Einführung der Governance, der Prozesse und Zuständigkeiten; Kommunikation und Steuerung der verschiedenen Ansprechpartner; Wahrnehmung von Schnittstellenfunktion; „Übersetzung“ der fachlichen Anforderungen in Konzepte und Technik

Am Beispiel für die Feststellung 1.21 (siehe nachfolgende Seite) kann durch KPMG wie folgt unterstützt werden:

Oft wird festgestellt, dass die fachliche Systemverantwortlichkeit für Anwendungen nicht eindeutig dokumentiert ist und nicht gelebt wird. So fehlen zum Beispiel notwendige Informationen bei Berechtigungsvergabe, Rezertifizierung oder Rollenbau. So besteht das Risiko, dass notwendige Prüfungen von Berechtigungen im jeweiligen System nicht erfolgen und unter Umständen zu Überberechtigungen führen. Dadurch sind Unternehmen nicht ausreichend vor Missbrauch und/oder Manipulation geschützt.

Ganz allgemein sind Voraussetzungen für ein funktionierendes Berechtigungsmanagement, unabhängig vom technischen Reifegrad einer IAM-Lösung im Unternehmen, die Definition und Beschreibung der Verantwortlichkeiten für Aufgaben und Tätigkeiten im Berechtigungsmanagement (BM). Als Basis dienen eine BM-Leitlinie, die Ausgestaltung im Standard „Verantwortlichkeiten im BM“ sowie das „Prozesshandbuch BM“. Dazu gehört auch die Festlegung und Dokumentation von Systemverantwortlichkeiten. Nur so kann gewährleistet werden, dass die jeweiligen Rezertifizierungen vollständig erfolgen.

Für die Feststellung 2.3 (siehe nachfolgende Seite) kann die Lösung durch KPMG wie folgt aussehen:

Häufig tritt der Sachverhalt in Unternehmen auf, dass hochprivilegierte Benutzerkonten von ganzen Teams verwendet werden können. Eine Attributierung einer Aktion zu einem konkreten Mitarbeiter ist nicht möglich. Dabei besteht das Risiko, dass ein Missbrauch oder eine falsche Verwendung des hochprivilegierten Users entstehen kann. Ein solcher Missbrauch gefährdet die Verfügbarkeit, die Integrität und die Vertraulichkeit der zugänglichen Unternehmensdaten. Wenn eine technische Lösung nicht möglich ist, sollte eine Prozessanweisung aufgesetzt werden, welche die Nutzung von hochprivilegierten Benutzern durch mehrere Personen untersagt. Die jeweilige Zuordnung und Nutzung durch einen Mitarbeiter kann per Dokumentation erfasst und kontrolliert werden. Des Weiteren sollte in einer Richtlinie die Vorgabe einer eindeutigen Verantwortlichkeit zu jedem hochprivilegierten Benutzer existieren.

Sind Sie an weiteren Lösungsansätzen interessiert bzw. wünschen einen Workshop zum Thema, kommen Sie gerne auf uns zu.

Feststellungen		
1.18	Es existiert kein Prozess, um sämtliche Berechtigungen eines Mitarbeiters zu sperren, der für längere Zeit abwesend bzw. pflichtabwesend ist.	**1 Access Administration**
1.19	Es existieren keine einheitlichen Antragsverfahren.	
1.20	Beantragte Zugriffsrechte werden ohne systematische Prüfung in die IT-Systeme eingegeben.	
1.21	Die fachliche Systemverantwortlichkeit für Anwendungen ist nicht eindeutig dokumentiert und wird nicht gelebt.	
2.3	Hochprivilegierte Benutzerkonten können von ganzen Teams verwendet werden. Eine Attribuierung einer Aktion zu einem konkreten Mitarbeiter ist nicht möglich.	**2 Identifikation und Authentifizierung**
2.4	Die Reichweite der Kenntnis des Passwortes von technischen Benutzerkonten im Unternehmen lässt sich abschließend nicht bestimmen.	
2.5	Die in der Kennwortrichtlinie festgelegten Anforderungen sind zu niedrig.	
2.6	Eine regelmäßige Passwortänderung wird nicht erzwungen.	
2.7	Es erfolgt keine individuelle Vergabe des Initialpassworts (z. B. Vergabe des aktuellen Monats, der aktuellen Jahreszeit, der Firma).	
3.7	Die Tätigkeiten der im IT-System hinterlegten technischen Benutzerkonten mit umfangreichen Berechtigungen werden nicht regelmäßig überwacht.	**3 Monitoring**
3.8	Technische Benutzerkonten sind nicht in den Rezertifizierungsprozess eingebunden.	
3.9	Die Rezertifizierung erstreckt sich nicht auf temporäre oder in Testumgebungen vergebene Zugriffsrechte.	
3.10	Die Zusammensetzung der Business-Rollen, deren Vergaberegeln bzw. die über sie außerhalb von Vergaberegeln berechtigten Benutzerkonten werden nicht in regelmäßigen Abständen rezertifiziert.	
3.11	Im Rezertifizierungsprozess werden nicht alle Akteure des Berechtigungsbeantragungs-Prozesses beteiligt.	
3.12	Es ist nicht sichergestellt, dass der Ist-Zustand im System dem Soll-Zustand im IAM-Tool entspricht. Es existieren keine regelmäßigen Consistency Maintenance-Prüfungen bzw. es ist nicht geregelt, wie mit Abweichungen umgegangen wird.	
4.2	Passwörter hochprivilegierter Benutzerkonten können von einzelnen Mitarbeitern ohne Wissen anderer Mitarbeiter bzw. ohne Kontrolle nach dem Vier-Augen-Prinzip geändert werden.	**4 Superuser**
4.3	Es ist nicht sichergestellt, dass die Nutzung eines privilegierten generischen Benutzer-kontos nach einer angemessenen Zeitdauer von zum Beispiel vier Stunden beendet wird.	
4.4	Es werden nicht überall, wo es möglich ist, personifizierte Administrator-Benutzerkonten eingesetzt.	

Feststellungen		
5.2	Es gibt keine übergreifenden Vorgaben zur Rollenmodellierung bzw. auch keine Vorgaben/Prozesse, wie Berechtigungsgruppen erstellt werden und diese einer Qualitätssicherung unterliegen.	**5 Vorgaben zur Berechtigungs-modellierung**
6.5	Es existiert keine vollständige, zentrale Übersicht über alle genutzten Anwendungen. Es kann daher nicht gewährleistet werden, dass alle Anwendungen angemessen in der Zugriffsrechteverwaltung erfasst sind.	**6 Berechtigungs-konzepte und deren Inhalte**
6.6	Die Prozesse zum Berechtigungsmanagement (insbesondere zur Beantragung und Genehmigung von Berechtigungen) sind in keiner/keinem unternehmensweiten Richtlinie bzw. Prozesshandbuch beschrieben.	
6.7	Die Berechtigungskonzepte werden nicht regelmäßig qualitätsgesichert.	

Ihre Ansprechpartner

KPMG AG
Wirtschaftsprüfungsgesellschaft
The SQUAIRE/Am Flughafen
60549 Frankfurt

Hans-Peter Fischer
Partner,
Consulting – Cyber Security
T +49 69 9587-2404
hpfischer@kpmg.com

Saskia Behrend
Senior Manager,
Consulting – Cyber Security
T +49 69 9587-4802
sbehrend@kpmg.com

Beta Systems IAM Software AG
Alt-Moabit 90 d
10559 Berlin

Detlef Sturm
Senior Business Consultant
T +49 30 726118 557
detlef.sturm@betasystems.com

www.kpmg.de

www.kpmg.de/socialmedia