# MaRisk-konformes Berechtigungsmanagement

## Ausgangssituation

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) formuliert in den Mindestanforderungen an das Risikomanagement (MaRisk) von Kredit- und Finanzdienstleistungsinstitutionen technisch-organisatorische Anforderungen wie folgt:

„Die IT-Systeme (Hardware- und Software-Komponenten), die zugehörigen IT-Prozesse und sonstige Bestandteile des Informationsverbundes müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen, insbesondere sind Prozesse für eine angemessene IT-Berechtigungsvergabe einzurichten, die sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt; die Zusammenfassung von Berechtigungen in einem Rollenmodell ist möglich. Die Eignung der IT-Systeme und der zugehörigen Prozesse ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.“ [MaRisk-Fassung vom 29.06.2023, AT 7.2, Tz. 2].

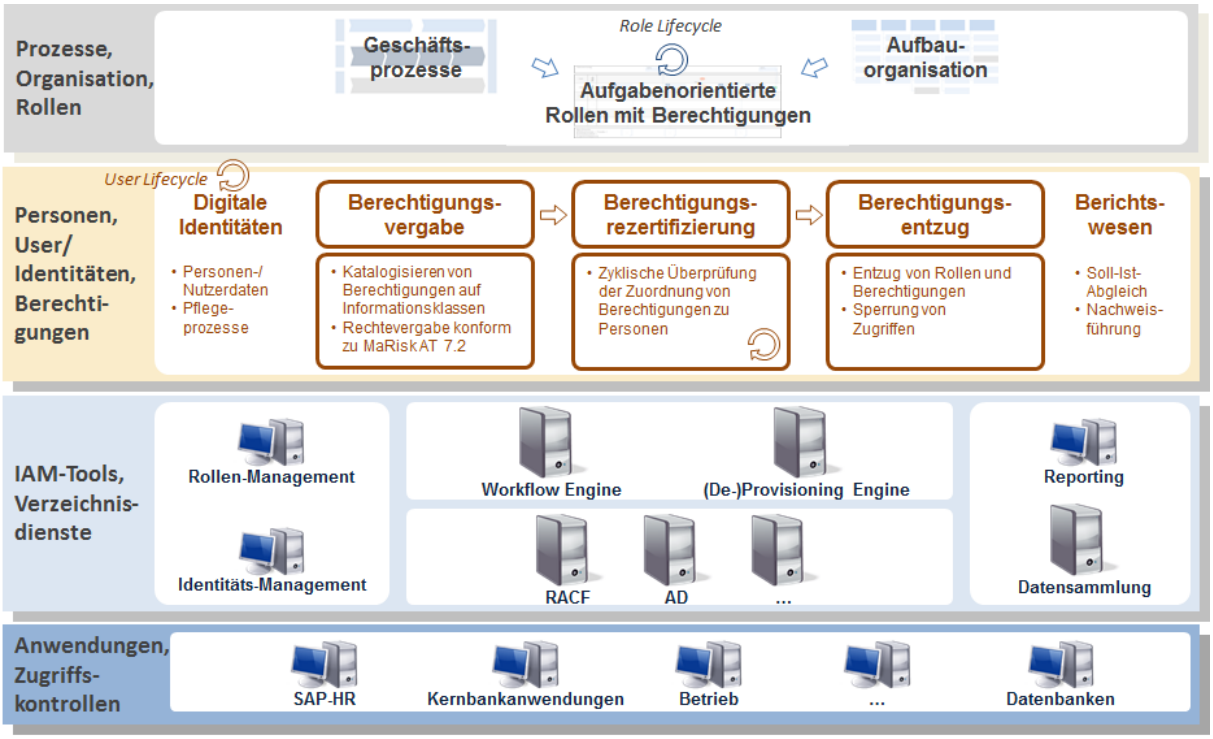
Um Informationen in Institutionen zu schützen, sollen Mitarbeiter nur die Zugriffsberechtigungen erhalten, die sie aufgrund übertragener Aufgabenverantwortungen begründet benötigen. So sollen z. B. nur Bankmitarbeiter Zugriffsberechtigungen auf Kundenkonten erhalten, wenn diese zur Erfüllung ihrer Aufgaben erforderlich sind. Zugriffe auf derart schützenswerte Informationen sind zu dokumentieren, um nachvollzogen werden zu können. Regelmäßig sind Aufgabenverantwortungen und vergebene Berechtigungen zu prüfen und bei weiterem Bedarf zu bestätigen (Rezertifizierung). Für ein effizientes Management der Berechtigungen können Aufgabenverantwortungen inklusive der notwendigen Berechtigungen zu organisatorischen Rollen zusammengefasst werden. Durch die Besetzung einer Rolle wie z. B. Kundenberater in einer Bank durch einen Mitarbeiter werden Aufgabenverantwortungen und die dazu notwendigen Berechtigungen für den Zugriff auf Informationen wie z. B. Kontostand und laufende Kredite zur Bonitätsprüfung vergeben.

In vielen Fällen stellt sich das Management von Zugriffsberechtigungen auf Informationen entgegen der BaFin-Vorgabe wie folgt dar: Das Berechtigungsmanagement orientiert sich an technischen, gewachsenen Berechtigungsstrukturen, oft individuell je nach System. Für neue Mitarbeiter oder neue Aufgaben müssen mehrere Berechtigungen für unterschiedliche Systeme getrennt beantragt werden. Die Berechtigungsvergabe wird durch Kopieren der Berechtigungen von einem Mitarbeiter zum anderen vorgenommen. Ein Zusammenhang zwischen Berechtigungen und Aufgabenverantwortung ist für viele Führungskräfte nicht nachvollziehbar. Vielfalt und Vielzahl von Systemen sowie Komplexität der technischen Strukturen führen dazu, dass regelmäßiges Überprüfen und ggf. Entziehen von Berechtigungen beim Wegfall von Aufgabenverantwortung vernachlässigt werden. In diesen Institutionen sammeln Mitarbeiter wie z. B. Trainees, die häufig Aufgaben wechseln und mehrere Abteilungen durchlaufen,

Berechtigung um Berechtigung. Dadurch steigt das Risiko eines unberechtigten Zugriffs auf schützenswerte Informationen.

## Ziele und Handlungsbedarf

Die Ziele der Kredit- und Finanzdienstleistungsinstitutionen in Bezug auf Berechtigungsmanagement sind die Erfüllung der MaRisk-Vorgabe AT 7.2 sowie die Etablierung effizienter Verfahren für Vergabe, Rezertifizierung und Entzug von Berechtigungen. Die folgende Abbildung schematisiert ein mögliches Zielbild für ein MaRisk-konformes und effizientes Berechtigungsmanagement.




Obiges Zielbild adressiert drei wesentliche Handlungsfelder:

1. **Soll-Berechtigungen für Aufgaben- bzw. Rollenverantwortungen:**
   Aus den Geschäftsprozessen und aufbauorganisatorischen Strukturen sind Aufgabenverantwortungen abzuleiten. Für die Wahrnehmung der Aufgabenverantwortungen sind notwendige und hinreichende Berechtigungen für den Zugriff auf Informationen und Systemfunktionen festzulegen. Werden Aufgaben zu organisatorischen Rollenverantwortungen zusammengefasst (Rollen-Management), können Berechtigungen effizient über die Rollen an Mitarbeiter vergeben und entzogen werden.

2. **Verfahren für Berechtigungsvergabe, -rezertifizierung und -entzug:**
   Für Vergabe, Rezertifizierung und Entzug von Berechtigungen sind Abläufe und Verantwortlichkeiten zu etablieren. Je nach Schutzbedarf der betroffenen Informationen sind ein- oder mehrstufige Genehmigungsverfahren sowie unterschiedliche Rezertifizierungsintervalle festzulegen. Vergaben, Rezertifizierungen sowie Entzüge sind für

eine Nachweisführung zu dokumentieren. Zur weiteren Effizienzsteigerung sind die Verfahren so weit wie möglich systemtechnisch zu unterstützen.

3. **Ist-Berechtigungen für Zugriffskontrolle auf Systeme und Informationen:** Anwendungen und Systeme mit zu schützenden Informationen sind in die Berechtigungsmanagementverfahren zu integrieren. Dabei sind systemorientierte Berechtigungsstrukturen mit aufgaben- bzw. rollenorientierten Strukturen zu verknüpfen. Durch regelmäßige Prüfungen sind Ist-Berechtigungen aus den Systemen mit den vordefinierten Soll-Berechtigungen abzugleichen. Bei Abweichungen sind Maßnahmen zur Anpassung der Ist-Berechtigungen an die Soll-Vorgaben durchzuführen.

Herausforderungen bei der Bearbeitung der Handlungsfelder verbergen sich gemäß unseren Projekterfahrungen in Abhängigkeiten von Handlungsfeldern zueinander und damit in der stufenweisen Erarbeitung des Zielbildes sowie in der Reichweite des Themas, welches sich integral wie ein Nervensystem durch einen Organismus durch nahezu alle Teile eines Unternehmens zieht und damit eine enge Abstimmung und Zusammenarbeit der beteiligten und betroffenen Organisationseinheiten erfordert. Dabei gilt es beispielsweise, die Sicht und Strukturen der Unternehmensorganisation mit der Vorstellung und Erfahrung der Informations- und Zielsystemverantwortlichen aufeinander abzustimmen und mit Blick auf das gemeinsame Zielbild zusammenzuführen.

Neben den Aspekten des Berechtigungsmanagements können sich für Kredit- und Finanzdienstleistungsinstitutionen bei der Auseinandersetzung mit IT-Risiken weitere Herausforderungen ergeben. Hierbei fordert die MaRisk-Vorgabe AT 7.2 die Verantwortlichen in diesen Institutionen auf, sämtliche informationstechnologische Risiken zu identifizieren und sich mit korrespondierenden Maßnahmen auf die Risikomitigation vorzubereiten. Obige Prozesse des Berechtigungsmanagements sowie die IT-Schutzmaßnahmen müssen auch auf Anwendungen, die der individuellen Datenverarbeitung zuzuordnen sind, übertragen werden.

## Unsere Leistungen

Gemeinsam mit Ihnen erarbeiten wir Ihr Zielbild für ein MaRisk-konformes **Berechtigungsmanagement** unter Berücksichtigung Ihrer Rahmenbedingungen. Vom aktuellen Berechtigungsmanagement in Ihrem Szenario ausgehend konkretisieren wir die Handlungsfelder in notwendige Arbeitspakte, welche in Abstimmung mit Ihnen in die Vorgehensweise zur Durchführung eines Projektes übernommen werden können.

Sowohl bei der Erstellung eines aufgaben- bzw. rollenorientierten Soll-Berechtigungskonzepts unter Einhaltung der Funktionstrennung als auch bei der Schaffung der organisatorischen Voraussetzungen zur Etablierung der Verfahren für die Vergabe, die Rezertifizierung und den Entzug von Berechtigungen begleiten wir Sie mit unserer Prozess- und Organisationsberatungskompetenz. Neben dem Aufbau eines nachhaltigen Rollen-Managements steht hierbei insbesondere die Besetzung der Verantwortlichkeiten entlang der Berechtigungsmanagementverfahren mit Führungskräften im Vordergrund.

Für die effiziente Durchführung des Berechtigungsmanagements leiten wir mit Ihnen Anforderungen an einzuführende, unterstützende Systemlösungen ab. Je nach Umfang und Ausbaustufe der gewünschten Systemunterstützung in Ihrem Szenario wählen wir mit Ihnen Lösungen aus, die von einer einfachen Excel-basierten Lösung bis hin zu hochintegrierten Produkten von Drittherstellern reichen.

Zusätzlich begleiten und unterstützen wir Sie bei der individuellen Konzeption und der Implementierung eines MaRisk-konformen **IT-Risikoschutzprozesses**. Darüber hinaus entwickeln wir für Sie Schutzmechanismen, die auch auf **Anwendungen individueller Datenverarbeitung** für ein angemessenes Niveau an Datensicherheit sorgen.

**Ihr Ansprechpartner:**
Dr. Christian Mayerl berät seit über 18 Jahren zu Strategien, Prozess- und Organisationsstrukturen für das Management der IT. Seine Erfahrungsschwerpunkte liegen insbesondere in den Branchen Finanzdienstleister, Automotive und IT-Dienstleister.

Telefon: +49 (89) 6137 283 – 0

E-Mail: info@mh-macon.de