IT-Berechtigungsmanagement

Vergabe und Kontrolle von IT-Berechtigungen

in der Reihe:

Bearbeitungs- und Prüfungsleitfaden

Prozesse prüfen * Risiken vermeiden * Fehler aufdecken
→ Handlungsempfehlungen ableiten

Finanz Colloquium Heidelberg, 2017

Zitiervorschlag:

Autor in: Bona-Stecki/Riediger/Uribe (Hrsg.), Bearbeitungs- und Prüfungsleitfaden: IT-Berechtigungsmanagement, RdNr. XX.

Download der Checklisten als Word-Dateien unter www.FC-Heidelberg.de
im persönlichen Benutzerbereich (Menüpunkt Mein FCH): **Zugangscode yEUg8**

ISBN: 978-3-95725-033-9

Finanz Colloquium Heidelberg GmbH
Im Bosseldorn 30, 69126 Heidelberg
www.FC-Heidelberg.de
info@FC-Heidelberg.de
Titelfoto: Silberberg GmbH Montafon
Satz: Finanz Colloquium Heidelberg GmbH
Druck: Digital Print Group O. Schimek GmbH, Nürnberg

Bearbeitungs- und Prüfungsleitfaden

IT-Berechtigungsmanagement

Vergabe und Kontrolle von IT-Berechtigungen

Mike Bona-Stecki (Hrsg.)
IT-Revisor, Interne Revision,
Sparkasse Langen-Seligenstadt

Roland Hein
Geschäftsführer,
bit Informatik GmbH

Andreas Kirsch
Management Consultant,
Security Assist GmbH

Andreas Kötter
Leiter Unternehmenssicherheit,
Volksbank Mittelhessen

Henning Riediger (Hrsg.)
Prüfungsleiter, Bankgeschäftliche Prüfungen,
Deutsche Bundesbank

Dr. Jaime Uribe (Hrsg.)
Geschäftsführer FCH Personal GmbH

Finanz Colloquium Heidelberg, 2017

Inhaltsübersicht

Inhaltsverzeichnis

A.

Aufsichtliche Anforderungen im Umgang mit Benutzerberechtigungen

A. Aufsichtliche Anforderungen im Umgang mit Benutzerberechtigungen[1]

I. Vorbemerkungen

Jeden Morgen (bei einigen sicherlich auch etwas später) beginnt für uns das Arbeitsleben im Büro zumeist mit dem Anmelden am »System«. Ein Benutzername und ein (hoffentlich korrektes) Passwort, und dem ersten Kaffee steht nichts mehr im Weg. Aber haben Sie sich bei diesem profanen Prozess eigentlich mal gefragt, welchen Zugang Sie mit ihrer Anmeldung jetzt bekommen haben? Wie hoch der Anteil der eingeräumten Rechte ist, die Sie täglich oder zumindest regelmäßig nutzen? Welche Rechte Sie haben, obwohl Sie die gar nicht benötigen? Oder welche Rechte Sie haben, die Sie gar nicht haben dürften? Typischerweise stellt man schnell fest, wenn man nicht alle Berechtigungen hat, die man benötigt. Anders herum kommt es doch eher sehr selten vor. 1

Und genau deswegen – dem Prinzip der minimalen Benutzerberechtigungen folgend – ist die Vergabe und Pflege von Benutzerberechtigungen ein zentrales Element des Internen Kontrollsystems in Banken und Sparkassen. 2

Die organisatorische Ausgestaltung von Kreditinstituten sollte immer unter der Maßgabe »Ohne die Informationstechnologie sind die Prozesse nichts, ohne die Prozesse ist die Informationstechnologie nichts!« beurteilt werden. Es wird sodann deutlich, dass die Informationstechnologie keinen Selbstzweck verfolgt, sondern mittlerweile **DIE elementare Grundlage** für das Betreiben des Bankgeschäfts ist. 3

Nicht nur die (Geschäfts-)Prozesse bedürfen einer regelmäßigen und angemessenen Überwachung, sondern auch die sie tragenden Komponenten der Informationstechnologie, an dieser Stelle maßgeblich über Benutzerberechtigungen. In der Praxis von Interesse ist vor allem die Diskussion über die Hierarchie von Schutzzielen von Relevanz. Es ist unstrittig, dass die Informationstechnologie möglichst jederzeit zur Verfügung stehen sollte. Um dieses Schutzziel zu erreichen, haben mithin viele Institute (oder deren Auslagerungsmandanten) erhebliche Ressourcen in die IT-Infrastruktur investiert. Derjenige der an dieser Stelle die Diskussion mit dem Verweis abbricht, alles 4

1 Die nachfolgenden Interpretationen und Meinungen sind ausschließlich persönliche Auffassungen des Verfassers und stellen keine offizielle Meinungsäußerung der Deutschen Bundesbank dar.

getan zu haben, droht zu ignorieren, dass sich die angemessene Steuerung und Überwachung operationeller Risiken im IT-Bereich nicht allein mit dem Schutzziel Verfügbarkeit erreichen lässt. Mindestens ebenso wichtig sind die weiteren Schutzziele Integrität, Authentizität und Vertraulichkeit der Daten. Was nützt es einem Institut auf verfügbaren Systemen zu arbeiten, wenn gleichzeitig nicht sichergestellt werden kann, dass die Veränderbarkeit von Daten in einem fest vordefinierten Umfeld erfolgt? Um dies zu vermeiden, müssen Schreib- (Integrität, Authentizität) und Leserechte (Vertraulichkeit) an Daten einem kontrollierten Benutzerberechtigungsvergabeprozess anhand eines Sollkonzeptes folgen. Die anschließende Überwachung in Form der Rezertifizierung der eingeräumten Benutzerberechtigungen ist eine nachgelagerte Kontrolle des Internen Kontrollsystems im IT-Bereich.

5 Unabhängig davon, wie gut die einzelnen Schutzziele verfolgt und erreicht werden, kann eine 100%ige Sicherheit – auch unter betriebswirtschaftlichen Aspekten – nicht erwartet werden, so dass die Geschäftsleitung eines Instituts permanent mit der Steuerung der verbleibenden operationellen (Rest-)Risiken konfrontiert ist.

6 Idealerweise fängt dies bereits in der Strategie mit der Definition von klaren überprüfbaren Aussagen an und leitet dann in den Informationsrisikomanagementprozess und den weiteren zentralen Komponenten wie Benutzerberechtigungen, Business Continuity Management und physische Sicherheit über. Aufgrund meiner Erfahrung aus Sonderprüfungen gemäß § 44 KWG komme ich zu dem Schluss, dass das Informationsrisikomanagement die tragende Säule des Internen Kontrollsystems im IT-Bereich ist und dass gerade bei Instituten, bei denen diese Komponente nicht angemessen ausgestaltet ist, grundlegende Probleme in den nachgelagerten Kontrollinstanzen – insbesondere bei Benutzerrechten – gehäuft auftreten.

7 In dem folgenden Buchbeitrag möchte ich Ihnen Anregungen für verschiedene Ausprägungen der Kontrollen im Internen Kontrollsystem des IT-Bereichs mit maßgeblichem Bezug zu Benutzerrechten aufzeigen, welche auch nach aufsichtlichem Verständnis geboten sind.

8 In der geplanten MaRisk-Novelle wird das Datenowner-Prinzip noch deutlicher als bisher betont. Galt bisher für die Einhaltung der Anforderungen an einen ordnungsgemäße Geschäftsorganisation i. S. s. § 25a Abs. 1 KWG maßgeblich der Gesamtvorstand (vgl. AT 3 Tz. 1 der MaRisk), so »ungeachtet der Gesamtverantwortung der Geschäftsleitung für die ordnungsgemäße Geschäftsorganisation und insbesondere für ein angemessenes und wirksames

Risikomanagement ist jeder Geschäftsleiter für die Einrichtung angemessener Kontroll- und Überwachungsprozesse in seinem jeweiligen Zuständigkeitsbereich verantwortlich.«[2] Dieser Verantwortung werden die jeweiligen Geschäftsleiter nur gerecht, wenn sie die Risiken beurteilen können und die erforderlichen Maßnahmen zu Ihrer Begrenzung treffen.

Angemessene Kontroll- und Überwachungsprozesse bestimmen sich an der angestrebten Risikokultur im Institut bzw. der Gruppe, welche sich aus den strategischen Vorgaben der Geschäfts- und Risikostrategie ableiten. Die Risikokultur beschreibt allgemein die Art und Weise, wie Mitarbeiter des Instituts im Rahmen ihrer Tätigkeiten umgehen sollen. Die Risikokultur soll die Identifizierung und den bewussten Umgang mit Risiken fördern und sicherstellen, dass Entscheidungsprozesse zu Ergebnissen führen, die auch unter Risikogesichtspunkten ausgewogen sind. Kennzeichnend für eine angemessene Risikokultur ist vor allem das klare Bekenntnis der Geschäftsleitung zu risikoangemessenen Verhalten, die strikte Beachtung des durch die Geschäftsleitung kommunizierten Risikoappetits durch alle Mitarbeiter und die Ermöglichung und Förderung eines transparenten und offenen Dialogs innerhalb des Instituts zu risikorelevanten Fragen.[3] 9

II. Grundsätzliche Überlegungen zum Management von IT-Risiken und Benutzerberechtigungen

Die Informationstechnologie (im Folgenden IT) leistet heutzutage einen nicht mehr wegzudenkenden und maßgeblichen Beitrag bei der Durchführung der Geschäftsprozesse in den Instituten. Nahezu alle wesentlichen Geschäftsprozesse werden durch IT-Komponenten und elektronisch gespeicherte Informationen unterstützt. Demnach kann die **Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 25a Abs. 1 KWG** eines Instituts nur unter der Einbeziehung und nach der Überprüfung der IT beurteilt werden. Um die Anforderungen an eine ordnungsgemäße Geschäftsorganisation zu erfüllen, wird als qualitative Aufsichtskomponente seit der Einführung der MaRisk im Jahr 2005 ein Risikomanagementprozess gefordert, in welchen entsprechend der geschilderten Relevanz auch die Benutzerberechtigungen einzubeziehen sind. Wem aber kommt in diesem Zusammenhang welche Aufgabe zu? 10

2 Vgl. AT 3 Tz. 2 der MaRisk (E).
3 Erläuterung zu AT 3 Tz. 1 MaRisk (E).

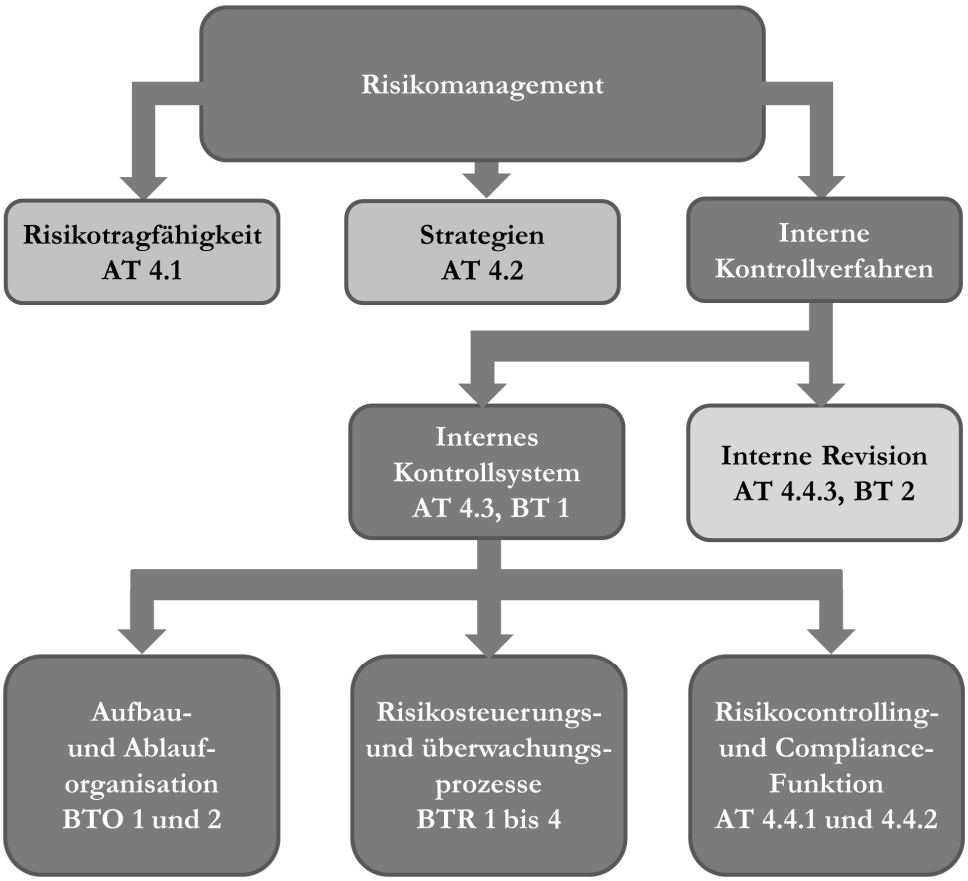

Abbildung 1: Hierarchie der MaRisk-Komponenten im Risikomanagement

11 Die MaRisk fordern den Aufbau Interner Kontrollverfahren, welche sich wiederum aus dem Internen Kontrollsystem und der Internen Revision zusammensetzen (vgl. Abb. 1). Die Aufgabe des Internen Kontrollsystems ist de facto die Kontrolle der eingerichteten Prozesse und Überwachungsaufgaben. Die Kontrollen dienen mithin dem Ziel Fehler, Schwachstellen und Mängel im Prozess transparent zu machen und dem Management die Möglichkeit zu bieten, korrigierend einzugreifen. Hingegen sollten die Aufgaben der Internen Revision sich darauf konzentrieren, zu beurteilen, ob das eingerichtete Interne Kontrollsystem funktionsfähig ist. Losgelöst von der idealtypischen Aufgabenverteilung ist in der Praxis häufig festzustellen, dass die eigentlich im Internen Kontrollsystem zu erwartenden Kontrollhandlungen durch die Interne Revision wahrgenommen werden. Derartige Funktionstrennungsverstöße führen im Ergebnis zu einer Einschränkung der Unabhängigkeit der Internen Revision, da die entsprechenden Prüfungshandlungen in der Folge entweder nicht mehr durchgeführt werden oder es aber zu einer nicht zweckmäßigen Überprüfung der eigenen Tätigkeiten kommt.

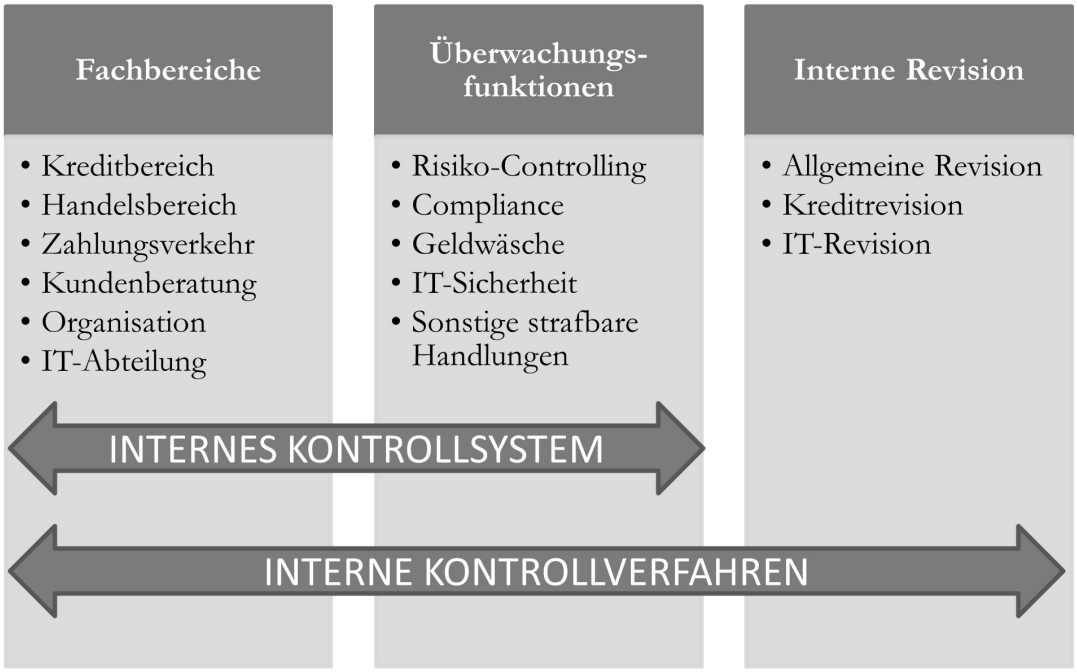

Abbildung 2: Konzept der drei Verteidigungslinien

Die Fachbereiche, welche das »Tagesgeschäft« mit den integrierten Kontrollen (z. B. Vier-Augen-Prinzip) abwickeln, stellen nach diesem Konzept die erste Verteidigungslinie dar. Die zweite Verteidigungslinie in Form der Überwachungs- bzw. Beauftragtenfunktionen soll sicherstellen, dass die eingerichteten Kontrollen wirksam und angemessen ausgestaltet sind. Über diese reine Kontrollfunktion hinaus sind die Funktionen auch an der Weiterentwicklung des Internen Kontrollsystem maßgeblich beteiligt bzw. notwendigerweise hinzuzuziehen. Die Einbindung kann sich über die Methodenentwicklung, die Durchführung von Prozessrisikoanalysen und letztendlich Beratung der Fachbereiche erstrecken. Ihnen kommt somit nicht nur eine reine Kontrollfunktion, sondern ebenso die Funktion eines Ideen- und Impulsgebers bzw. Optimierers zu. Für den IT-Bereich des Internen Kontrollsystems sind hierbei vor allem der IT-Sicherheitsbeauftragter sowie auch der Compliance-Beauftragte gefordert. In einem weiteren Schritt, wenn es insgesamt um die gesamtweite Beurteilung der bestehenden bzw. eingegangenen Risikopotenziale geht, kommt das Risiko-Controlling hinzu. 12

13 Welche Aufgaben hierbei zu berücksichtigen sind, soll die folgende Abbildung verdeutlichen:

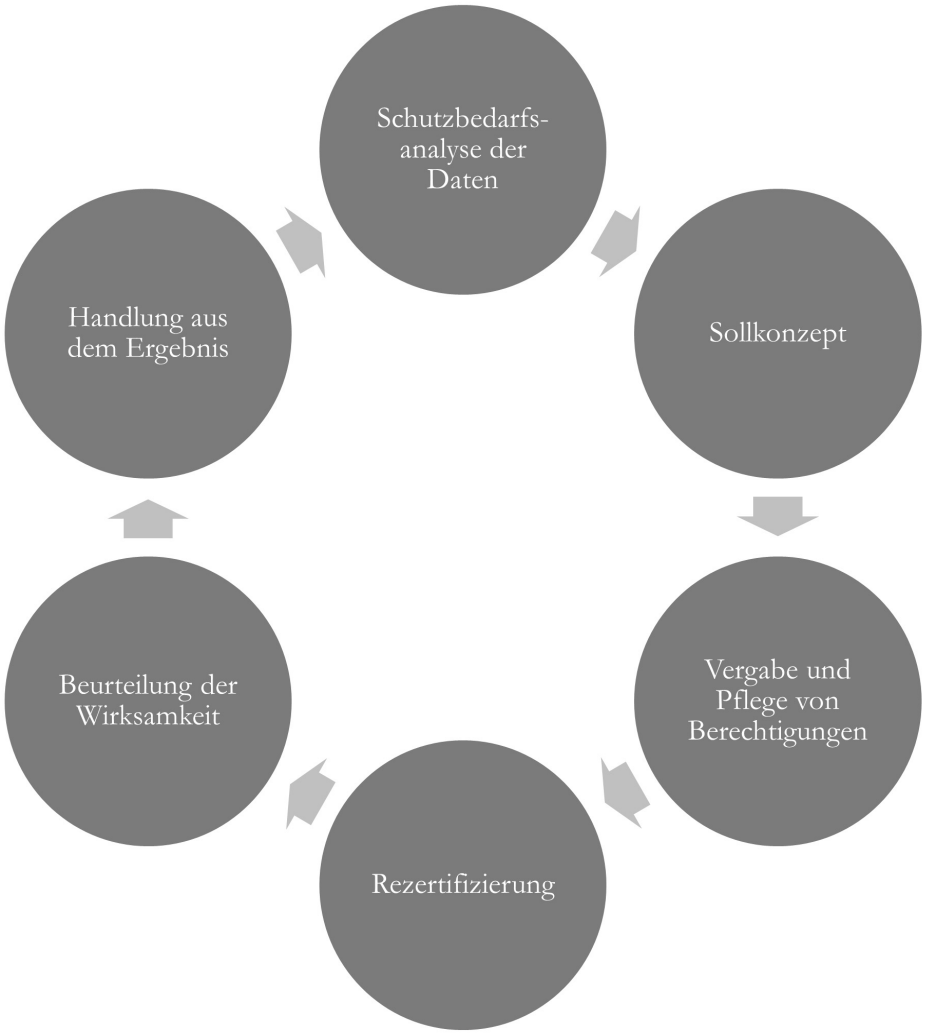

Abbildung 3: Kreislauf der Überprüfung der Benutzerberechtigungen

14 Die Interne Revision – hierbei im Fokus natürlich die IT-Revision – stellt eine unabhängige Überprüfungsinstanz dar. Dieser Grundsatz – fest vorgegeben als prozessunabhänige Abteilung gemäß AT 4.4.3 Tz. 3 der MaRisk – wird jedoch in der Praxis nicht immer komplett in ausreichendem Maße sichergestellt. So muss als Ergebnis aus Bankgeschäftlichen Prüfungen gemäß § 44 KWG häufiger festgestellt werden, dass das Aufgabenspektrum der Interne Revision respektive die aktuelle Handhabung im Institut deutlich in den Bereich des Internen Kontrollsystems hineinreicht und damit Bestandteil des Prozesses wird. Typische Fälle sind die Einbindung in die revisionsseitige Abnahme von Sollkonzepten, Einzelberechtigungen und der Prozess der Rezertifizierung.

Zur Veranschaulichung ein paar Beispiele aus der Praxis: 15

- Bearbeitung von Auslegungsfragen zum Sollkozept,
- Freigabe des Sollkonzepts,
- Rechtliche Beurteilung von Vorgängen,
- Abnahme von Individueller Datenverarbeitung,
- Durchführung der Rezertifizierung von Benutzerberechtigungen,
- Erstellen und/oder Freigabe von Organisationsrichtlinien für die Administration und Benutzerberechtigungsvergabe,
- Durchführung der Auslagerungsüberwachung im Sinne des Internen Kontrollsystems und
- Auditing und Monitoring bestimmter Administrationstätigkeiten bzw. Nutzung bestimmter Rechte mit Zugriff auf besonders relevante Daten.

Alle diese geschilderten Fälle haben einen gravierenden Mangel gemeinsam: es 16
kann in der Folge **keine unabhängige Prüfung** durch die Interne Revision erfolgen. Das in der Folge häufig angeführte Argument, es müsse in der Folge lediglich Personenidentität ausgeschlossen werden, reicht nach gängiger aufsichtlicher Auslegungspraxis nicht aus, da die daraus resultierenden Interessenskonflikte und teilweise ebenso Interessensidentitäten diese Vorgehensweise als nicht angemessen im Sinne der Funktionstrennung nach MaRisk qualifizieren.

1. Strategische Vorgaben zum Umgang mit Risiken aus IT

Der Einstieg in das Risikomanagement im Bereich IT wird durch die strategi- 17
schen Vorgaben des Instituts determiniert. Derlei übergeordnete Sollvorgaben definieren die Ziele und Rahmenbedingungen der einzelnen Institute und bilden die Grundlage für die darauf aufbauende operative Planung und Umsetzung. Hierfür ist es erforderlich, dass die strategischen Vorgaben hinreichend konkret sind und entsprechend objektiv überprüfbare Aussagen enthalten. Nur wenn eine valide Aussage über die Einhaltung der strategischen Sollvorgaben möglich ist, kann der Gesamtprozess des Risikomanagements im IT-Bereich funktionieren.

Hierzu in der Folge ein Beispiel: Ein Institut gibt in den **strategischen Vor-** 18
gaben an, dass in den nächsten Jahren, dem Horizont der mittelfristigen Geschäftsplanung, die Kosten im IT-Bereich gesenkt werden sollen. Allerdings ist hierbei im Nachgang zu hinterfragen, was unter dieser Aussage zu verstehen ist und inwieweit die Aussage objektiv überprüfbar ist. Kann – provokant gefragt – die strategische Vorgabe der Kostensenkung bereits erreicht werden,

wenn eine Tastatur weniger beschafft wird als geplant? Es fehlt demnach an der Ableitung einer objektiv überprüfbaren Aussage. Somit wäre zu benennen, in welchen Bereichen diese Maßnahmen durchgeführt werden und in welchem Umfang diese aufweisen sollen.

19 Die Umsetzung der Strategie muss also klar aufzeigen, ob die potenziellen Einsparungen den IT-Personalbereich, die Beschaffung von Hard- und Software oder letztendlich die IT-Sicherheit treffen sollen. Vor dem Hintergrund stetig steigender Personalkosten im IT-Bereich und aufgrund der Tatsache, dass die fortlaufende Sicherstellung der Innovationsfähigkeit bei der Bereitstellung entsprechender IT-Komponenten, lässt sich offensichtlich nicht erwarten, dass es in diesen Bereichen nennenswerte potenzielle Einsparungsmöglichkeiten geben kann. Betrachtet man dann die verbleibenden Optionen, kann nur die IT-Sicherheit als Sparbereich identifiziert werden. Ist das Institut bestrebt dort Einsparungen vorzunehmen, muss dies dann jedoch in den strategischen Vorgaben ersichtlich und transparent für alle Empfänger sein.

20 Beispielsweise ist es hilfreich das Prinzip der minimalen Berechtigungsvergabe bereits in den strategischen Vorgaben zu verankern. Nur allein die Erwähnung reicht natürlich nicht aus. Vielmehr sollte eine Aussage getroffen, ab welchem Schutzniveau der Daten ein entsprechendes Benutzerberechtigungskonzept erforderlich ist.

21 Die getroffenen Vorgaben müssen somit die vom Institut angestrebte und akzeptierte Risikotoleranz abbilden. Hierbei muss anerkannt werden, dass auch bei einer vollständigen Erfüllung der strategischen Vorgaben Restrisiken im Institut verbleiben und in Kauf genommen werden müssen, die nicht explizit und aktiv gesteuert werden können. Welche Restrisiken dies sein können, muss im Rahmen der Risikoinventur gemäß AT 2.2 der MaRisk ermittelt werden.

22 Es stellt sich jedoch regelmäßig die Frage, wie mit **Restrisiken** umzugehen ist, nachdem sie durch die Risikoinventur – beispielsweise in Form eines Self-Assessments – transparent geworden sind? Die Kernfrage sollte dann immer lauten, welche Auswirkung hätte ein Schlagendwerden des betrachteten Risikoereignisses auf die Vermögens-, Ertrags- und Liquiditätslage? Die Risikoereignisse sind jedoch zunächst brutto zu betrachten und erst in einem zweiten Schritt anhand der Einbindung in den Risikomanagementprozess zu bewerten. Es ist zu erwarten, dass es entsprechende geschäftspolitische Entscheidungen gibt, wie mit solchen Risiken bzw. Risikoclustern umzugehen ist.