ORO make regulation work

Severn make change work

_ Whitepaper

Rundschreiben zur VAIT-Novelle 2022: Neuerungen der IT-Regulierung für Versicherungen

Endfassung der VAIT-Novelle 2022 zeigt umfangreichen Handlungsbedarf für betroffene Institute auf – keine Umsetzungsfrist für die Institute

Severn Consultancy GmbH, Hansa Haus, Berner Str. 74, 60437 Frankfurt am Main, www.severn.de

Inhaltsverzeichnis

1 Management Summary

Sofortige Umsetzung

Das Rundschreiben 10/2018 (VA) in der Fassung vom 03. März 2022 für die „versicherungsaufsichtlichen Anforderungen an die IT (VAIT)“ wurde aktuell veröffentlicht. Es sind keine Umsetzungsfristen vorgesehen. Daher gilt die sofortige Umsetzung der Anforderungen der VAIT. Für die Institute bedeutet dies einen hohen Umsetzungsdruck, denn die Jahresabschlussprüfer werden bereits im Jahresabschluss 2022 zum Umsetzungsstand der neuen VAIT berichten; die Berichte gehen automatisch zur Aufsicht. Gleichzeitig stellt der Themenbereich der IT neben dem Adressenausfallrisiko einen der zentralen Themenschwerpunkte für IT-Sonderprüfungen dar. Die einzelnen Vorstände haben die zügige Umsetzung zu verantworten.

Einsatz von Informationstechnik

Der Einsatz von Informationstechnik (IT), auch unter Einbeziehung von IT-Services, die durch IT-Dienstleister bereitgestellt werden, hat eine zentrale Bedeutung für Versicherungsunternehmen und Pensionsfonds. Die VAIT enthalten vielfältige Hinweise zur Auslegung der Vorschriften über die Geschäftsorganisation im Versicherungsaufsichtsgesetz (VAG), soweit sie sich auf die technisch-organisatorische Ausstattung der Unternehmen beziehen. Sie legt diese Vorschriften für die BaFin verbindlich aus und gewährleistet hierdurch eine konsistente Anwendung gegenüber allen Unternehmen und Gruppen. Hierbei wurden auch Erfahrungen aus bankaufsichtlichen Prüfungen mit berücksichtigt.

Neuerungen im Kurzüberblick

Organisatorisch wurde das frühere Kapitel 5 „Benutzerberechtigungsmanagement“ in die zwei neuen Kapitel 5 „Operative Informationssicherheit“ und Kapitel 6 „Identitäts- und Rechtemanagement“ aufgeteilt. Mit dem Kapitel 10 „IT-Notfallmanagement“ kommt ein neues Kapitel hinzu, welches die Ausführungen zur Notfallplanung ergänzt.

Wesentliche Änderungen beinhalten die neuen Anforderungen an das Informationsrisikomanagement (IRM) mit internen Kontrollen zur Überprüfung der Angemessenheit und Wirksamkeit der Maßnahmen zum Schutz der Informationen, welche zukünftig zu planen und durchzuführen sind. Das Informationssicherheitsmanagement (ISM) muss in Zukunft unter anderem die Wirksamkeit der bestehenden Kontrollen aus der “First-Line-of-Defence", d.h. der operativen Informationssicherheit, nachweisen. Auch für den IT-Betrieb steigen insgesamt die Anforderungen an eine notwendige Transparenz sowie den Dokumentationsbedarf der eingesetzten IT-Komponenten. Weiterhin ist auch die Verbesserung bestehender und die Etablierung zusätzlicher IT-Betriebsprozesse, etwa zur Steuerung von Verfügbarkeit und Kapazitäten, notwendig.

Es ist eine beobachtete Tendenz in VAIT-bezogenen IT-Sonderprüfungen, dass die Aufsicht eine starke Ausrichtung an „Blueprint“-Lösungen mit Qualitätsanforderung „best-of-class“ fordert und weniger den proportionalitätsbezogenen Umsetzungsansatz begrüßt. Dies bedeutet auch ein „Revival“ des BSI-Grundschutzes als Orientierungspapier und konkrete Handlungsvorgabe für die IT-Umsetzung in den einzelnen Instituten.

Die neue Version der VAIT beinhaltet weitere Verschärfungen im Bereich der Informationssicherheit, wie die erstmals formulierte „Operative Informationssicherheit“, die die

Aufgabenbereiche der First-Line-of-Defence von den Bereichen der Second-Line wie Informationsrisikomanagement und Informationssicherheitsmanagement deutlicher abgrenzt und zu einer Stärkung der betrieblichen Kontrollfunktionen und damit einer wirksamen Funktionstrennung insgesamt führt.

Durch das neue Kapitel 5 „Operative IT-Sicherheit“ wurden bisherige Anforderungen an Netzwerksicherheit, Systemhärtung, Penetrations- und Schwachstellentests verschärft und konzentriert.

Mit dem Kapitel 10 „IT-Notfallmanagement“ sind Ziele zum Notfallmanagement zu definieren und hieraus abgeleitet ein Notfallmanagementprozess aufzusetzen. Für alle IT-Systeme, welche zeitkritische Aktivitäten und Prozesse unterstützen, sind IT-adäquate Notfallpläne zu erstellen. Die IT-Notfallpläne umfassen Wiederanlauf-, Notbetriebs- und Wiederherstellungspläne sowie die dafür festgelegten Parameter und berücksichtigen Abhängigkeiten, um die zeitkritischen Aktivitäten und Prozesse wiederherzustellen. Neben der schnellen Wiederfortführung der kritischen Geschäftsprozesse stehen auch wirksame Notfallübungen im Fokus der Regulierung.

Die bestehenden Kapitel der VAIT wurden in verschiedenen Bereichen weiter konkretisiert oder zum Teil auch inhaltlich erweitert bzw. modifiziert.

Handlungsbedarf

Durch die Neuregelungen resultiert für die betroffenen Institute **erheblicher Handlungsbedarf** in nahezu **allen wesentlichen IT-Bereichen** der Institute. Um schnell und zuverlässig einen **transparenten Überblick** über den erforderlichen Anpassungsbedarf aus der VAIT-Novelle zu erhalten, bieten Severn und ORO **strukturierte und praxiserprobte Lösungsansätze.** Severn und ORO kombinieren dabei fachliche IT-Expertise und methodische Erfahrung – nachgewiesen in zahlreichen Projekten für renommierte Banken und Finanzdienstleistungsgesellschaften.

2 Neuerungen der VAIT-Novelle

Die modulare Struktur der VAIT wurde erweitert, bestehende Vorgaben konkretisiert und neue Anforderungen aufgenommen:

Modul VAIT	Erweiterte bzw. neue Anforderung
I Vorbemerkung	*Proportionalität* – Das Rundschreiben gibt einen flexiblen und praxisnahen Rahmen vor, insbesondere für das Management der IT-Ressourcen, für das Informationsrisikomanagement und das Informationssicherheitsmanagement. *Regelungsbereich* – Betroffen sind alle nach § 1 Abs. 1 VAG der Aufsicht unterfallenden Unternehmen mit Ausnahme der Versicherungs-Zweckgesellschaften im Sinne des § 168 VAG und der Sicherungsfonds im Sinne des § 223 VAG. Das Rundschreiben betrifft auch Unternehmensgruppen, wenn alle gruppenzugehörigen Erst- und Rückversicherungsunternehmen ihren Sitz im Inland haben. *Anwendung auf Unternehmensgruppen* – Es gilt zudem für Gruppen mit Erst- oder Rückversicherungsunternehmen in anderen Mitglieds- oder Vertragsstaaten gemäß § 7 Nr. 22 VAG, für die nach den in § 279 Abs. 2 VAG genannten Kriterien die BaFin die für die Gruppenaufsicht zuständige Behörde ist. – Alle der Gruppenaufsicht unterworfenen Unternehmen haben bei der Erfüllung der Anforderungen auf Gruppenebene mitzuwirken (§ 246 Abs. 3 VAG). Dabei sind insbesondere die Grundsätze des § 275 VAG zu beachten. Der in diesem Rundschreiben verwendete Begriff „Unternehmen“ schließt die Gruppen mit ein. *MaGo/ EbAV* – Für Unternehmen, die den Anwendungsbereichen der Rundschreiben 02/2017 „Aufsichtsrechtliche Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo)“, 08/2020 „Aufsichtsrechtliche Mindestanforderungen an die

	Geschäftsorganisation von Einrichtungen der betrieblichen Altersvorsorge (MaGo für EbAV)" sowie 01/2020 „Aufsichtsrechtliche Mindestanforderungen an die Geschäftsorganisation von kleinen Versicherungsunternehmen nach § 211 VAG (MaGo für kleine VU)" unterliegen, bleiben die in den jeweiligen Rundschreiben enthaltenen Anforderungen unberührt und werden im Rahmen ihres Gegenstandes durch dieses Rundschreiben konkretisiert. Unternehmen haben auch bei Ausgliederungen an IT-Dienstleister durch angemessene Regelungen in der Ausgliederungsvereinbarung die Einhaltung der Anforderungen aus diesem Rundschreiben durch den IT-Dienstleister sicherzustellen. IT-Dienstleister im Sinne dieses Rundschreibens können auch Trägerunternehmen von EbAV sein. *Orientierung an gängige IT-Standards* – Die Themenbereiche dieses Rundschreibens sind nach Regelungstiefe und -umfang nicht abschließender Natur. Das Unternehmen bleibt folglich auch insbesondere jenseits der Hinweise in diesem Rundschreiben gemäß den Anforderungen an die Geschäftsorganisation im VAG verpflichtet, bei der Ausgestaltung der IT-Systeme (Hardware- und Software-Komponenten) und der dazugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Zu diesen zählen beispielsweise der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik und die internationalen Sicherheitsstandards ISO/IEC 270XX der International Organization for Standardization. *Nutzung des Proportinalitätsprinzips* – Bei der Umsetzung der Anforderungen an die Geschäftsorganisation und somit auch der Ausgestaltung der Strukturen, IT-Systeme oder Prozesse können Erleichterungen genutzt werden. Die Anforderungen sind auf eine Weise zu erfüllen, die der Wesensart, dem Umfang und der Komplexität der mit der Tätigkeit des Unternehmens einhergehenden Risiken (im Weiteren „Risikoprofil") gerecht wird (§ 296 Abs. 1 VAG). Orientierungsgrößen sind dabei das individuelle Risikoprofil, die geringe Größe sowie die Mitarbeiterzahl. – Die Proportionalität wirkt sich darauf aus, wie Anforderungen erfüllt werden können. So können bei Unternehmen mit schwächer ausgeprägtem Risikoprofil einfachere Strukturen, IT-Systeme oder Prozesse ausreichend sein. Umgekehrt kann das Proportionalitätsprinzip bei Unternehmen mit stärker ausgeprägtem Risikoprofil aufwändigere Strukturen, IT-Systeme oder Prozesse erfordern. – Die Einschätzung, welche Gestaltung als proportional anzusehen ist, ist in Bezug auf das einzelne Unternehmen nicht statisch, sondern passt sich im Zeitablauf den sich verändernden Gegebenheiten an. In diesem Sinne haben die Unternehmen und Gruppen zu prüfen, ob und wie die vorhandenen Strukturen, IT-Systeme oder Prozesse weiterentwickelt werden können und ggf. müssen. *Ordnungsgemäße Geschäftsorganisation* – Alle Geschäftsleiter eines Unternehmens sind für eine ordnungsgemäße und wirksame Geschäftsorganisation gesamtverantwortlich. Soweit sich die Anforderungen dieses Rundschreibens auf die Geschäftsleitung beziehen, ist immer die gesamte Geschäftsleitung gemeint. Diese kann insofern ihre Gesamtverantwortung nicht delegieren, auch nicht auf einen oder mehrere Geschäftsleiter.
Kapitel 1 – IT-Strategie	– **1.1** / Künftig muss die **Geschäftsleitung** für die **Umsetzung** der **IT-Strategie** Sorge tragen. Die Geschäftsleitung hat zur Überwachung und Messung der Umsetzung von Zielen, Strategie sowie zu ihrer Beurteilung und Anpassung einen Prozess einzurichten. – **1.2** Ziffer a) / Bei der IT-Aufbau- und Ablauforganisation sind künftig wichtige **Abhängigkeiten** von **Dritten** zu berücksichtigen. In den Erläuterungen zu Ziffer a) wurden die möglichen sonstigen **wichtigen Abhängigkeiten** von Dritten (wie z.B. Informations-, Telekommunikations- und Versorgungsdienstleistungen etc.) ergänzt. – **1.2** Ziffer b) / Bei der Zuordnung der gängigen Standards, auf die das Unternehmen abstellt, wurde neben den Bereichen der IT auch der Bereich der **Informationssicherheit** ergänzt. – **1.2** Ziffer c) / Neben den bisherigen Zuständigkeiten und der Einbindung der Informationssicherheit in die Organisation wurden auch die **Ziele** der **Informationssicherheit** in der IT-Strategie aufgenommen. In den Erläuterungen zur Ziffer c) ist eine Erweiterung bezüglich der grundlegenden Aussagen zur **Schulung** und **Sensibilisierung** zur **Informationssicherheit** aufgenommen worden, denn ohne die ständige Schulung und Sensibilisierung ist keine Kontinuität der Informationssicherheit sicherzustellen. – **1.2** Ziffer e) / Die Aussagen zum IT-Notfallmanagement wurden unter Berücksichtigung der **Informationssicherheitsbelange** erweitert. Dies betrifft auch die Ergänzungen zur operativen Informationssicherheit in dem neuen Kapitel 5 der VAIT. – **1.5** / Die Inhalte sowie Änderungen der IT-Strategie sind innerhalb des Unternehmens künftig auch „**zeitnah**" und in geeigneter Weise zu kommunizieren.
Kapitel 2 – IT-Governance	– **2.1** / Bei den Vorgaben zur IT-Aufbau- und IT-Ablauforganisation, zum Informationsrisiko- sowie Informationssicherheitsmanagement wurden die Angaben zur quantitativ und qualitativ angemessenen **Ressourcenausstattung** der IT (personelle, finanzielle und sonstige Ressourcen) ergänzt bzw. spezifiziert. Weiterhin wurden die früheren Regelungen durch **Leitlinien** für die IT-Aufbau- und IT-Ablauforganisation ersetzt. Die IT-Governance soll künftig in Form von Leitlinien vorgegeben werden. – In den Erläuterungen zu 2.1 wurde ergänzt, dass die Vorgaben zur IT-Governance künfig Bestandteil regelmäßiger Überprüfungen durch hinreichend **qualifizierte interne Revisoren** sind. Dies erweitert die Prüfungsaufgaben der Internen Revision und stellt auch Anforderungen an die qualifizierte Ausbildung der IT-Revisoren. – **2.4** / Das Unternehmen hat insbesondere das Informationsrisikomanagement, das Informationssicherheitsmanagement, den IT-Betrieb und die Anwendungsentwicklung quantitativ und qualitativ angemessen mit **Ressourcen** auszustatten. Auch hierbei wurde die Personalausstattung in Ressourcen umgewandelt. Bei der Bewertung der **Ressourcenausstattung** (**personelle, finanzielle und sonstige Ressourcen**) werden insbesondere der Stand der Technik sowie die aktuelle und zukünftige Bedrohungslage berücksichtigt. – **2.8** / Zur Steuerung der für den Betrieb und die Weiterentwicklung der IT-Systeme zuständigen Bereiche durch die Geschäftsleitung sind angemessene quantitative oder qualitative Kriterien durch diese festzulegen. Die Einhaltung der **Kriterien** ist zu überwachen und wurde damit nochmals präzisiert.

Kapitel 3 – Informations-risiko-management	– **3.1** Kommentierung / Die Risikokriterien berücksichtigen jetzt auch die Kritikalität der Geschäftsprozesse und -aktivitäten sowie bekannte Gefährdungen und Vorfälle, welche das Unternehmen bereits in der Vergangenheit beeinflusst haben. – **3.2** Kommentierung / Die Risikokriterien berücksichtigen künftig auch die **Kritikalität der Geschäftsprozesse** und -**aktivitäten** sowie bekannte **Gefährdungen** und **Vorfälle**, welche das Unternehmen bereits in der Vergangenheit beeinflusst haben. – **3.3** / Zu den maßgeblichen Stellen gehören auch die Fachbereiche, die Eigentümer der Informationen oder – neu eingefügt – Eigentümer der **Informationsrisiken** sind. – **3.4** / Zu einem **Informationsverbund** gehören beispielsweise geschäftsrelevante Informationen, Geschäfts- und Unterstützungsprozesse, IT-Systeme und die zugehörigen IT-Prozesse sowie Netz- und Gebäudeinfrastrukturen. Künftig sind auch Abhängigkeiten und Schnittstellen zu berücksichtigen wie auch die Vernetzung des Informationsverbundes mit Dritten. – **3.5** / Das Unternehmen hat regelmäßig und anlassbezogen den **Schutzbedarf** für die Bestandteile seines definierten Informationsverbundes, insbesondere im Hinblick auf die Schutzziele „Integrität", „Verfügbarkeit", „Vertraulichkeit" und „Authentizität") zu ermitteln. Die Eigentümer der Informationen bzw. die Fachbereiche, die verantwortlich für die Geschäftsprozesse sind, **verantworten** die **Ermittlung** des **Schutzbedarfs**. – **3.5** / Die **Schutzbedarfsfeststellung** sowie die zugehörige Dokumentation sind durch das Informationsrisikomanagement angemessen zu überprüfen. – **3.8** / Das Unternehmen hat auf Basis der festgelegten Risikokriterien künftig **regelmäßig** eine Risikoanalyse durchzuführen. Die Risikoanalyse ist zu **koordinieren** und zu **dokumentieren**. – **3.9** / Das Unternehmen hat sich nun auch über laufende **Bedrohungen** und **Schwachstellen** seines Informationsverbundes zu informieren, die Relevanz zu prüfen und die Auswirkung zu bewerten. Sofern erforderlich, sind geeignete technische und organisatorische Maßnahmen zu ergreifen. Hierbei sind interne und externe Veränderungen (z.B. der **Bedrohungslage**) zu berücksichtigen. – **3.10** / Kommentierung – Der Statusbericht enthält die Risikosituation des Unternehmens und künftig auch Informationen über **externe potenzielle Bedrohungen**.

Kapitel 4 – Informations-sicherheits-management

- **4.2** / In der Kommentierung zu 4.2 wurden auch verschiedene Punkte ergänzt bzw. präzisiert. In der **Informationssicherheitsleitlinie** werden die Eckpunkte zum Schutz von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität sowie der Geltungsbereich für die Informationssicherheit festgelegt. Darüber hinaus werden die wesentlichen organisatorischen Aspekte, wie - neu eingefügt - die wichtigsten Rollen und Verantwortlichkeiten des **Informationssicherheitsmanagements** beschrieben. Mit der Leitlinie legt die Geschäftsleitung u.a. folgende neu eingeführten Kriterien dar:
  - ihre Gesamtverantwortung für die Informationssicherheit,
  - Frequenz und Umfang des Berichtswesens zur Informationssicherheit,
  - die Kompetenzen im Umgang mit Informationssicherheitsrisiken,
  - die grundlegenden Anforderungen der Informationssicherheit an Personal, Auftragnehmer, Prozesse und Technologien,
  - geeignete Kriterien für die Information der Geschäftsleitung über Informationssicherheitsvorfälle, sofern diese Kriterien nicht in einer Informationssicherheitsrichtlinie dargelegt werden.
- Die Aufsicht hat die **Verantwortung** der **Geschäftsleitung** für die Informationssicherheitsleitlinie nochmals herausgestellt und die Bedeutung des Managements von Informationssicherheitsrisiken hervorgehoben. Es wird hier auch stärker auf die Kollektivverantwortung für IT und IT-Sicherheit durch die gesamte Geschäftsleitung hingewiesen.
- **4.3** / Kommentierung / Informationssicherheitsrichtlinien werden z.B. für die Bereiche Netzwerksicherheit, Kryptografie, Identitäts- und Rechtemanagement, Protokollierung sowie **physische Sicherheit** (z.B. Perimeter- und Gebäudeschutz) erstellt. Neu dabei ist die Ergänzung bezüglich des Identitäts- und Rechtemanagements sowie des **Perimeter-** und **Gebäudeschutzes**. Damit wurde klargestellt, dass sowohl der systemseitige Zugriff als auch der physische Zutritt, z.B. zum Rechenzentrum, ein originäres Thema der Informationssicherheit und in den Richtlinien explizit zu regeln ist. Ergänzt wurde auch, dass zu den Ergebnissen des Informationsrisikomanagements u.a. die definierten Sollmaßnahmen (vgl. 3.7) zählen.
- **4.4** / Neu aufgenommen ist das Erfordernis, dass das Unternehmen eine **Richtlinie** über das **Testen** und **Überprüfen** der **Maßnahmen** zum **Schutz** der **Informationssicherheit** einzuführen und diese regelmäßig und anlassbezogen zu überprüfen und bei Bedarf anzupassen hat. Die ausreichende Qualifikation der Tester ist zu gewährleisten. Die Richtlinie berücksichtigt u.a.:
  - die allgemeine Bedrohungslage,
  - die individuelle Risikosituation des Unternehmens,
  - Kategorien von Test- und Überprüfungsobjekten (z.B. das Unternehmen, IT-Systeme, Komponenten),
  - Art, Umfang und Frequenz von Tests und Überprüfungen,
  - Zuständigkeiten und Regelungen zur Vermeidung von Interessenkonflikten.
- Die neue Erfordernis der „Richtlinie über das Testen und Überprüfen der Maßnahmen zum **Schutz** der **Informationssicherheit**" zeigt, dass die Aufsicht einen klar hinterlegten Regelprozess und mit der Richtlinie klare Tests und die regelmäßige Überprüfung der Maßnahmen der Informationssicherheit fordert. Diese sollen an der jeweiligen Bedrohungslage des Instituts abgeleitet werden, d.h. Szenarien für das Institut sind festzuschreiben und auf die Tests, Maßnahmen und Kontrollen sowie den Turnus der Überwachung auszurichten.
- **4.5** / Neu ist, dass die Geschäftsleitung die Funktion des Informationssicherheitsbeauftragten einzurichten hat. Weiterhin wurden die Aufgaben der Funktion des Informationssicherheitsbeauftragten präzisiert:
  - die Beteiligung bei der Erstellung und Fortschreibung des Notfallkonzepts bzgl. der Informationssicherheitsbelange,
  - angemessene Beteiligung bei Projekten und Beschaffungen mit IT-Relevanz (je nach Einzelfall kann eine angemessene Beteiligung reichen von der Information des Informationssicherheitsbeauftragten über das IT-Projekt bis hin dazu, dass der Informationssicherheitsbeauftragte das IT-Projekt überwacht und auf Einhaltung der Informationssicherheit hinwirkt)
- Künftig kann der Informationssicherheitsbeauftragte auch durch ein **Informationssicherheitsmanagement-Team** unterstützt werden.
- **4.6** / In der Kommentierung zu 4.6 wurden zur Funktion des Informationssicherheitsbeauftragten weitere Konkretisierungen vorgenommen. Zur Vermeidung möglicher Interessenkonflikte werden zudem insbesondere folgende neue Maßnahmen beachtet:
  - Funktions- und Stellenbeschreibung für den Informationssicherheitsbeauftragten, seinen **Vertreter** und ggf. **weitere Stellen**
  - ein der Funktion zugewiesenes Budget für Informationssicherheitsschulungen im Unternehmen und die persönliche Weiterbildung des Informationssicherheitsbeauftragten sowie seines Vertreters und ggfs. des Informationssicherheitsmanagement-Teams
- **4.8** / Nach einem **Informationssicherheitsvorfall** sind die Auswirkungen auf die Informationssicherheit nun zeitnah zu analysieren und angemessene Nachsorgemaßnahmen zu veranlassen.
- In der Prüfungspraxis kam es immer wieder zu Auffälligkeiten, da ein **Informationssicherheitsvorfall** nicht immer als solcher transparent erkennbar war, sondern in der Regel eine Evolution aus sicherheitsrelevantem Ereignis(sen) darstellt, die als solche nachvollziehbar erkannt werden muss. Hierzu ist ein umfängliches und automatisiertes SIEM (Security Information and Event Management) erforderlich. Dabei ist der Einsatz eines IT-Tools unerlässlich. Es sollte auch der teils hohe Implementierungsaufwand des Tools mit berücksichtigt werden.
- Die Definition des Begriffes „Informationssicherheitsvorfall" wurde konkretisiert. Danach orientieren sich die betroffenen Bestandteile des Informationsverbundes nach Art und Umfang des Schutzbedarfs. Ein Informationssicherheitsvorfall kann auch dann vorliegen, wenn mindestens eines der Schutzziele („Verfügbarkeit", „Integrität", „Vertraulichkeit", „Authentizität") gemäß den Vorgaben des institutsspezifischen Sollkonzepts der Informationssicherheit verletzt ist.
- Die Aufsicht fordert von den Instituten eine transparente Abgrenzung der Begriffe **Informationssicherheitsvorfall** und **normale Störung**. Hier gab es in der bisherigen Prüfungspraxis Überschneidungen. Die Aufsicht möchte jedoch eine „klare Abgrenzung". Auch eine Aggregation von Störungen kann zu Informationssicherheitsvorfällen führen.

  4.9 / Das Institut hat nun auch ein kontinuierliches und angemessenes **Sensibilisierungs-** und **Schulungsprogramm** für **Informationssicherheit** festzulegen. Der Erfolg der festgelegten Sensibilisierungs- und Schulungsmaßnahmen ist zu überprüfen. Das Programm sollte zielgruppenorientiert mindestens folgende Aspekte berücksichtigen:

  - persönliche Verantwortung für eigene Handlungen und Unterlassungen sowie allgemeine Verantwortlichkeiten zum Schutz von Informationen
  - grundsätzliche Verfahren zur Informationssicherheit (wie Berichterstattung über Informationssicherheitsvorfälle) und allgemeingültige Sicherheitsmaßnahmen (z.B. zu Passwörtern, Social Engineering, Prävention vor Schadsoftware und dem Verhalten bei Verdacht auf Schadsoftware)
- Die Aufsichtspraxis zeigt, dass das Thema der Informationssicherheit oft immer noch eher als „lästige Pflicht" angesehen wird. Daher wird eine wirksame Schulung und Sensibilisierung mit einer Erfolgsmessung nachgefordert (Regelkreislauf). Jeder Mitarbeiter ist dabei aufgerufen, sich aktiv an den Maßnahmen zur Informationssicherheit zu beteiligen. Die Prüfungspraxis zeigt auch, dass die Aufsicht ebenfalls Vorstände und Aufsichtsräte hier stärker in die Pflicht nimmt, da das relevante Wissen im Kontext der Informationssicherheit oft nicht ausreichend vorhanden ist.

5. Operative Informations-sicherheit	– **5.1** / In dem neuen Kapitel 5 soll die **operative Informationssicherheit** die Anforderungen des Informationssicherheitsmanagements operativ umsetzen. IT-Systeme, 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. Für **IT-Risiken** sind angemessene Überwachungs- und Steuerungsprozesse einzurichten, die insbesondere die Festlegung von IT-Risikokriterien, die Identifikation von IT-Risiken, die Festlegung des Schutzbedarfs, daraus abgeleitete Schutzmaßnahmen für den IT-Betrieb sowie die Festlegung entsprechender Maßnahmen zur Risikobehandlung und –minderung umfassen. Bei dem Thema der operativen IT-Sicherheit ziehen die Anforderungen weiter an. Es soll in der Praxis durchgesetzt werden, dass die Ausgangsbasis der Schutzbedarfsanalyse/ Risikoanalyse und die abgeleiteten Maßnahmen wirkungsvoll in der **Prozess-** und **Kontrolllandkarte** der Institute umgesetzt werden. – In der Prüfungspraxis liegen klar beschriebene Prozesse zur Erstellung und Fortschreibung von wichtigen Liefergegenständen der Informationssicherheit oft nicht vor. Die Liefergegenstände gibt es i.d.R., jedoch ist deren Erstellung und Weiterentwicklung eher ad-hoc erfolgt und folgt (noch) nicht einem „Regelbetrieb" mit klaren Schritten, Verantwortlichkeiten und verlässlichen Verfahren. – **5.2** / Das Institut hat nun auch auf Basis der Informationssicherheitsleitlinie und Informationssicherheitsrichtlinien angemessene, dem Stand der Technik entsprechende, **operative Informationssicherheitsmaßnahmen** und **Prozesse** zu implementieren. Informationssicherheitsmaßnahmen und -prozesse berücksichtigen u.a.: – Schwachstellenmanagement zur Erkennung, Bewertung, Behandlung und Dokumentation von Schwachstellen – Segmentierung und Kontrolle des Netzwerks (einschließlich Richtlinienkonformität der Endgeräte) – Sichere Konfiguration von IT-Systemen (Härtung) – Verschlüsselung von Daten bei Speicherung und Übertragung gemäß Schutzbedarf – Mehrstufigen Schutz der IT-Systeme gemäß Schutzbedarf (z.B. vor Datenverlust, Manipulation oder Verfügbarkeitsangriffen oder vor nicht autorisiertem Zugriff) – Perimeterschutz von z.B. Liegenschaften, Rechenzentren und anderen sensiblen Bereichen – Die Auswahl der beispielhaft genannten Themen korreliert sehr stark mit Erkenntnissen aus der aufsichtlichen Prüfungspraxis. Aus diesem Grund sind in der Praxis die inhaltlichen Erwartungen an die Professionalität der geforderten Lösungsbausteine sehr hoch. Hierbei besteht hochgradige Prüfungsrelevanz (auch in der IT-Vorprüfung zum Jahresabschluss, also auch in jährlichem Turnus). – **5.3** / Künftig sind die **Gefährdungen** des **Informationsverbundes möglichst frühzeitig** zu identifizieren. Potentiell sicherheitsrelevante Informationen sind angemessen, zeitnah, regelbasiert und zentral auszuwerten. Diese Informationen müssen bei Transport und Speicherung geschützt werden und für eine angemessene Zeit zur späteren Auswertung zur Verfügung stehen. – Potentiell **sicherheitsrelevante Informationen** sind z.B. Protokolldaten, Meldungen und Störungen, welche Hinweise auf Verletzung der Schutzziele geben können. Die regelbasierte Auswertung (z.B. über Parameter, Korrelationen von Informationen, Abweichungen oder Muster) großer Datenmengen erfordert in der Regel den Einsatz automatisierter IT-Systeme. Spätere Auswertungen umfassen u.a. forensische Analysen und interne Verbesserungsmaßnahmen. Der Zeitraum sollte der Bedrohungslage entsprechend bemessen sein. – Es wird die Einführung einer umfassenden und automatisierten SIEM-Lösung gefordert, über welche regelmäßige Auswertungen gefahren werden, um Hinweise für die Verletzung der Schutzziele zu ermitteln. Dies ist eine neue Qualität der Überwachung. In der Praxis wird die Umsetzung durchweg mit höheren Kosten verbunden sein. Eine solche SIEM-Lösung erfordert auch automatisierte Zuliefersysteme z.B. aus dem Identity- und Access Management sowie aus PAM und dem Change Management. Es entsteht somit ein hoher aufsichtlicher Evolutionsdruck auf die gesamte Datenverarbeitungskette und das IT-Compliance Management. – **5.4** / Es ist ein angemessenes Portfolio an Regeln zur Identifizierung sicherheitsrelevanter Ereignisse zu definieren. Diese Regeln sind vor Inbetriebnahme zu testen und regelmäßig und anlassbezogen auf Wirksamkeit zu prüfen und weiterzuentwickeln. – Regeln erkennen beispielsweise, ob vermehrt nicht autorisierte Zugriffsversuche stattgefunden haben, erwartete Protokolldaten nicht mehr angeliefert werden oder die Uhrzeiten der anliefernden IT-Systeme voneinander abweichen. Die Regeln müssen dazu geeignet sein, anomale Aktivitäten und Bedrohungen zu erkennen. – Weiter beschäftigt sich der Abschnitt mit der Parametrierung der SIEM-Lösung und schreibt ein „angemessenes" Set an sogenannten „Use Cases" vor, welche durch die Regel-Engine des SIEM automatisch abgeprüft wird. Die Angemessenheit muss sich am Bedrohungspotential und Schutzbedarf ausrichten und verdeutlicht die zunehmende „integrierte Systematisierungsabsicht" der Aufsicht. – **5.5** / **Sicherheitsrelevante Ereignisse** sind zeitnah zu analysieren und auf daraus resultierende Informationssicherheitsvorfälle ist unter Verantwortung des Informationssicherheitsmanagements angemessen zu reagieren. Diese Ereignisse ergeben sich beispielsweise aus der regelbasierten Auswertung der potentiell sicherheitsrelevanten Informationen. Die zeitnahe Analyse und Reaktion kann eine ständig besetzte zentrale Stelle, z.B. in Form eines Security Operation Centers (SOC), erfordern. – Die Aufsicht möchte eine zeitnahe Analyse der sicherheitsrelevanten Ereignisse, damit eventuelle Sicherheitslücken schnell geschlossen werden. Hierfür müssen die organisatorischen Voraussetzungen geschaffen werden. Auch muss eine kompetente Interventionsstrategie für das SOC/CERT bestehen, damit strukturiert gegen den Angriff auf die Schutzziele reagiert werden kann. – **5.6** / Künftig ist die **Sicherheit** der **IT-Systeme** regelmäßig, anlassbezogen und unter Vermeidung von Interessenkonflikten zu überprüfen. Die Ergebnisse sind hinsichtlich notwendiger Verbesserungen zu analysieren und Risiken angemessen zu steuern. Für kritische Systeme hat die Überprüfung mindestens jährlich zu erfolgen. – Turnus, Art und Umfang der Überprüfung sollten sich insbesondere am Schutzbedarf und der potentiellen Angriffsfläche (z.B. Erreichbarkeit aus dem Internet) des IT-Systems orientieren. Arten der Überprüfungen sind z.B.: Abweichungsanalysen (Gap-Analysen), Schwachstellenscans, Penetrationstests und Simulationen von Angriffen. – Hierbei fordert die Aufsicht eine regelmäßige und anlassbezogene Sicherheitsüberprüfung der IT-Systeme. Einige Unternehmen lassen die IT-Sicherheit von externen Firmen prüfen inkl. der Penetrationstests. Wichtig für die Umsetzung wäre die Festlegung der Verfahren sowie die ausreichende Dokumentation. Als Ausblick ist hier zu nennen, dass die europäische Aufsicht stark auf eine weitere Professionalisierung dieser Penetrationstests dringt (TIBER Initiative); insofern muss das Thema ernsthaft umgesetzt werden. Das **Schwachstellenmanagement** steht auch sehr stark im Prüfungsfokus und muss heutzutage durch professionelle und aktuelle Tools vorgenommen werden (z.B. Qualys, Nessus). Damit direkt verbunden ist ein (tages-)aktuelles Patchmanagement, um die Schwachstellen zu beseitigen. Die Prüfungspraxis zeigt hier regelmäßig Defizite auf.

6. Identitäts- und Rechte-management	– **6.1** / Das alte Kapitel Benutzerberechtigungsmanagement wurde inhaltlich ergänzt und in **Identitäts-** und **Rechtemanagement** umbenannt – die internen Kontrollanforderungen wurden erweitert. Das neue Identitäts- und Rechtemanagement stellt sicher, dass den Benutzern eingeräumte Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben des Instituts entspricht. Bei der Ausgestaltung des Identitäts- und Rechtemanagements sind die Anforderungen an die Ausgestaltung der Prozesse (siehe 2.2 und 2.10) entsprechend zu berücksichtigen. Jegliche Zugriffs-, Zugangs- und Zutrittsrechte auf Bestandteile bzw. zu Bestandteilen des Informationsverbundes sollten standardisierten Prozessen und Kontrollen unterliegen. – Die wesentliche Neuerung liegt in den standardisierten Prozessen und **Kontrollen** der **Zugriffs-, Zugangs- und Zutrittsrechte** auf die Bestandteile des Informationsverbundes. Die nachfolgenden Detailanforderungen lassen sich ohne eine automatisierte IAM-Lösung nicht mehr prüfungsfest umsetzen. – **6.2** / Die **Inhalte** der **Berechtigungskonzepte** wie Umfang und Nutzungsbedingungen der Berechtigungen wurden um Zugang zu IT-Systemen, Zugriff auf Daten sowie Zutrittsrechte zu Räumen erweitert. Diese sind konsistent zum ermittelten **Schutzbedarf** sowie vollständig und nachvollziehbar ableitbar für alle bereitgestellten Berechtigungen festzulegen. Berechtigungskonzepte haben die Vergabe von Berechtigungen nach dem Sparsamkeitsgrundsatz („Need-to-Know" und „Least-Privilege" Prinzipien) sicherzustellen, die Funktionstrennung auch berechtigungskonzeptübergreifend zu wahren und Interessenkonflikte zu vermeiden. Berechtigungskonzepte sind regelmäßig und anlassbezogen zu überprüfen und ggf. zu aktualisieren. Neu ergänzt wurde in der Kommentierung auch die folgende Anforderung: Zugangs- und Zugriffsberechtigungen auf den IT-Systemen können auf allen Ebenen eines IT-Systems (z.B. Betriebssystem, Datenbank, Anwendung) vorliegen. – Im Rahmen des Sparsamkeitsgrundsatzes sind auch die Zugriffsrechte jedes einzelnen technischen Benutzers auf das unbedingt erforderliche Minimum zu beschränken und nicht benötigte Benutzerkonten zu löschen. – Eine mögliche Nutzungsbedingung ist die Befristung der eingeräumten Berechtigungen. Berechtigungen sollten je nach Art für personalisierte sowie für nicht personalisierte Benutzer (inkl. technische Benutzer) vorliegen. Technische Benutzer sind z.B. Benutzer, die von IT-Systemen verwendet werden, um sich gegenüber anderen IT-Systemen zu identifizieren oder um eigenständig IT-Routinen auszuführen. – Die Aufsicht präzisiert die Anforderungen an die Berechtigungskonzepte als Basis und Dokumentations-Golden Source aller Aspekte von Berechtigungen für IT-Assets (Achtung: Nicht mehr nur Applikationen, sondern auch die tieferen Ebenen des Technologie-Stacks, so z.B. auch wichtige Infrastruktur-Komponenten). Hier wird viel Prüfungspraxis aufgegriffen. Ein weiterer Aspekt ist die geforderte übergreifende Funktionstrennung, welche z.B. auch für Funktionen im Technologie-Stack gilt (z.B. Datenbank-Admin versus Applikations-Admin). – **6.3** / Neu ist die Ergänzung, dass **Zugriffe** und **Zugänge** jederzeit zweifelsfrei einer handelnden bzw. verantwortlichen Person (möglichst automatisiert) zugeordnet werden müssen. Beispielsweise müssen automatisierte Aktivitäten den verantwortlichen Personen zuordenbar sein. Abweichungen in begründeten Ausnahmefällen und die hieraus resultierenden Risiken sind zu bewerten, zu dokumentieren und anschließend von der fachlich verantwortlichen Stelle zu genehmigen. – Die Aufsicht präzisiert die Anforderungen an die nicht personalisierten User wie Root- oder Test-User etc. Es muss lückenlos nachvollziehbar sein, wer diese in welchem Umfang benutzt hat, bzw. die Risiken müssen von den Entscheidungsträgern übernommen werden (z.B. bei Einsatz Root-User). Dies erfordert i.d.R. den Einsatz einer hinreichend komplexen PAM-Lösung mit Passwort-Vault und ggfs. Session Recording. – **6.4** / Die bisherige Erläuterung in der Kommentierung zu 6.4, d.h. Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen umfasst jeweils auch die zeitnahe oder unverzügliche Umsetzung im Zielsystem und wurde um eine Erläuterung ergänzt. U.a. stellt die Gefahr einer missbräuchlichen Verwendung von Berechtigungen einen Grund für eine unverzügliche Deaktivierung oder Löschen ebendieser Berechtigungen dar. – **6.5** / Kommentierung: Fällt im Rahmen der Rezertifizierung auf, dass nicht legitimierte Berechtigungen vorhanden sind, so werden diese gemäß Regelverfahren zeitnah entzogen und bei Bedarf weitere Maßnahmen (z.B. Ursachenanalyse, Vorfallmeldung) ergriffen. – Die Einführung der "**unverzüglichen Deaktivierung**" bedeutet in der gelebten Prüfungspraxis „taggleiche Deaktivierung". Diese Vorgabe gilt für sämtliche Systeme auf die der Mitarbeiter Zugriff hat. Dies gilt übrigens auch bei „Movern" also Abteilungs- oder Stellenwechsel eines Mitarbeiters. – **6.7** / Folgende Formulierung wird nun in den neuen BAIT erläutert. Das Institut hat nach Maßgabe des Schutzbedarfs und der Soll-Anforderungen **Prozesse** zur **Protokollierung** und **Überwachung** einzurichten, die überprüfbar machen, dass die Berechtigungen nur wie vorgesehen eingesetzt werden. Denn aufgrund der damit verbundenen weitreichenden Eingriffsmöglichkeiten hat das Institut insbesondere für die Aktivitäten mit privilegierten (besonders kritischen) Benutzer- und Zutrittsrechten angemessene Prozesse zur Protokollierung und Überwachung einzurichten. – Die Aufsicht fordert, dass die Berechtigungen generell risikoorientiert gesondert zu überwachen sind. Neben der Identifizierung sind angemessene Prozesse und Überwachungsmaßnahmen erforderlich. Dies erfordert PAM-Verfahren, welche auch privilegierte Business-Nutzer umfassen (z.B. Freigaben hoher Beträge). Bislang beschränkte sich PAM auf administrative Nutzer. Die Ausweitung auf physischen Zutritt erfordert für Unternehmen ein automatisiertes Zutrittsmanagement und greift hier in die Gebäudetechnik ein. – Die übergeordnete Verantwortung für die Prozesse zur Protokollierung und Überwachung von Berechtigungen wird nach wie vor einer Stelle zugeordnet, die unabhängig vom berechtigten Benutzer oder dessen Organisationseinheit ist. Neu ist die Regelung, dass zu privilegierten Zutrittsrechten in der Regel die Rechte zum Zutritt zu Rechenzentren, Technikräumen sowie sonstigen sensiblen Bereichen zählen. – **6.8** / Kommentierung: Bei den technisch-organisatorischen Maßnahmen gab es einige Ergänzungen: – Bei der Auswahl angemessener Authentifizierungsverfahren wurden u.a. starke Authentifizierung im Falle von Fernzugriffen aufgenommen sowie – die automatische passwortgesicherte Bildschirmsperre aufgenommen.

7. IT-Projekte und Anwendungsent-wicklung	– **7.2** / Weiter konkretisiert wurden die Produktionsumgebungen. Diese sind grundsätzlich voneinander in **Entwicklungs-** und **Testumgebungen** zu trennen. – **7.3** / Kommentierung: Bei den Erläuterungen zum erstmaligen Einsatz sowie für wesentliche Veränderungen wurde der Begriff „IT-Systeme" in **Anwendungen** ersetzt. – **7.4** / Kommentierung: Die Erfordernisse von IT-Projekten wurden weiter spezifiziert. Danach zählen nun zu den notwendigen **organisatorischen Grundlagen** u.a.: – Einbindung betroffener Beteiligter (insbesondere des Informationssicherheitsbeauftragten) – Projektdokumentation (z.B. Projektantrag, Projektabschlussbericht) – Quantitative und qualitative Ressourcenausstattung – Steuerung der Projektrisiken – Informationssicherheitsanforderungen – Projektunabhängige Qualitätssicherungsmaßnahmen – Aufarbeitung der gewonnenen Erkenntnisse (Lessons Learned) – **7.5** / IT-Projekte sind unter Berücksichtigung ihrer Ziele und Risiken im Hinblick auf die Dauer, Ressourcen und ihre Qualität angemessen zu steuern. Werden im Rahmen von IT-Projekten größere Änderungen an Prozessen mit Auswirkungen auf die **Informationssicherheit** erforderlich, sind entsprechende Änderungsanträge zu stellen und zu bearbeiten. Hierfür sind Vorgehensmodelle festzulegen, deren Einhaltung zu überwachen ist. – **7.6 /** keine Änderungen – **7.7** / Kommentierung: Bei den Erläuterungen zur Berichterstattung an die Geschäftsleitung über IT-Projekte und IT-Projektrisiken wurden lediglich redaktionelle Anpassungen vorgenommen. – **7.8** / Die Anwendungsentwicklung umfasst u.a. die Erstellung von Software für Geschäfts- und Unterstützungsprozesse (einschließlich individueller Datenverarbeitung – IDV). – **7.9** / Sowohl Anforderungen an die Funktionalität der Anwendung wie auch nichtfunktionale Anforderungen müssen erhoben, bewertet und dokumentiert werden. Zu jeder Anforderung sind entsprechende Akzeptanz- und Testkriterien zu definieren. Die Verantwortung für die Erhebung und Bewertung der Anforderungen (funktional und nicht funktional) haben die fachlich verantwortlichen Stellen zu tragen. – Anforderungsdokumente können sich nach Vorgehensmodell unterscheiden und beinhalten bspw.: – Fachkonzept (Lastenheft) – Technisches Fachkonzept (Pflichtenheft) – User Story – **7.10** / Je nach Schutzbedarf sind im Rahmen der Anwendungsentwicklung angemessene Vorkehrungen zu treffen, dass auch im produktiven Vertrieb einer Anwendung die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten nachvollziehbar sichergestellt werden. – Zu den geeigneten Vorkehrungen zählen: – Die Prüfung der Eingabedaten – Systemzugangskontrolle – Benutzerauthentifizierung – Transaktionsautorisierung, Protokollierung der Systemaktivität – Prüfpfade (Audit Logs) – Verfolgung von sicherheitsrelevanten Ereignissen – Behandlung von Ausnahmen – **7.11** / Die Integrität der Anwendung (insbesondere des Quellcodes) ist angemessen sicherzustellen. Als zusätzliche Anforderungen wurde festgelegt, dass Vorkehrungen getroffen werden müssen, die erkennen lassen, ob eine Anwendung versehentlich geändert oder absichtlich manipuliert wurde. – Als geeignete Vorkehrung definiert die VAIT bspw. die Überprüfung des Quellcodes als methodische Untersuchung zur Identifizierung von Risiken. – **7.12** / Die Anwendungsentwicklung (von Dritten, aber auch eigene durchgeführte) ist für sachkundige Dritte nachvollziehbar zu dokumentieren. – Sie muss dabei folgende Mindestinhalte bieten: – Anwenderdokumentation – Technische Systemdokumentation – Betriebsdokumentation – **7.13** / Für das Testen von Anwendungen vor ihrem erstmaligen Einsatz und nach wesentlichen Änderungen ist eine Methodik zu definieren und einzuführen. Die Tests haben in ihrem Umfang die Funktionalität der Anwendung und die implementierten Maßnahmen zum Schutz der Informationen einzubeziehen. Die Durchführung von fachlichen Abnahmetests verantworten die fachlich zuständigen Stellen. – Die Testdurchführung erfordert einschlägige Expertise der für den Test verantwortlichen Personen. Weiterhin müssen diese Personen in ihrer Tätigkeit unabhängig von den Anwendungsentwicklern sein. Der Schutzbedarf der zum Test verwendeten Daten ist zusätzlich zu berücksichtigen. – Sofern der Schutz der Informationen dies erfordert, sind Penetrationstests in die Testaktivitäten mit einzubeziehen. – **7.14** / Kommentierung: Eine redaktionelle Anpassung bei der das Wort „der" durch „einer" ersetzt wurde. – **7.15** / Kommentierung: Mehrere redaktionelle Anpassungen. – **7.16** / Kommentierung: Eine redaktionelle Anpassung bei der das Wort „Endbenutzern" durch „Mitarbeitern" ersetzt wurde.

8. IT-Betrieb	_ **8.2** / Kommentierung: Die Mindestinhalte der Bestandsangaben zu Komponenten der IT-Systeme wurden um „Eigentümer der IT-Systeme und deren Komponenten" sowie „Schutzbedarf und Kritikalitätseinstufung der IT-Systeme und deren Komponenten" erweitert. _ **8.3** / Das Portfolio aus IT-Systemen bedarf der Steuerung. IT-Systeme sollten regelmäßig aktualisiert werden. Risiken aus veralteten bzw. nicht mehr vom Hersteller unterstützten IT-Systemen sind zu steuern (Lebenszyklus-Management). Nicht mehr verwendete Hardwarekomponenten sind sicher zu entsorgen. _ Zu den Hardwarekomponenten zählen neben den Rechnern insbesondere auch die Datenträger. _ **8.4** / Die Aufsicht bestimmt, dass „Änderungen von IT-Systemen" auch eine Wartung von IT-Systemen beinhaltet. _ Weiterhin wurden verschiedene redaktionelle Änderungen vorgenommen. _ **8.5** / Änderungen von IT-Systemen und größere Prozessänderungen mit Auswirkungen auf die Informationssicherheit sind zu beantragen. Auch für zeitkritische Änderungen von IT-Systemen sind geeignete Prozess einzurichten. _ Zudem wurden redaktionelle Änderungen vorgenommen. _ **8.6** / Für Störungsmeldungen sind Standardvorgehensweisen z.B. für Maßnahmen und Kommunikation sowie Zuständigkeiten (z.B. für Schadcode auf Endgeräten, Fehlfunktionen) zu definieren. Weiterhin sind geeignete Kriterien für die Information der Beteiligten (z.B. Geschäftsleitung, zuständige Aufsichtsbehörde) über Störungen festzulegen. _ **8.7** / Die Verfahren zur Wiederherstellung und zur Gewährleistung der Lesbarkeit der Daten sind regelmäßig, mindestens jährlich, im Rahmen einer Stichprobe sowie anlassbezogen zu testen. _ Die Anforderungen an die Ausgestaltung der entsprechenden Maßnahmen ergeben sich aus den zugrundeliegenden Risikoanalysen. _ **8.8** / Der aktuelle Leistungs- und Kapazitätsbedarf der IT-Systeme ist zu erheben. Der zukünftige Leistungs- und Kapazitätsbedarf ist abzuschätzen. Die Leistungserbringung ist zu planen und zu überwachen um insbesondere Engpässe zeitnah zu erkennen und angemessen zu reagieren. Bei der Planung sind Leistungs- und Kapazitätsbedarf von Informationssicherheitsmaßnahmen zu berücksichtigen.
9. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen	_ **9.2** / In Bezug auf jede sonstige Dienstleistungsbeziehung im Bereich der IT-Dienstleistungen, haben betroffene Unternehmen vorab eine Erhebung und Bewertung von funktionalen und nicht funktionalen Anforderungen sowie eine Risikoanalyse durchzuführen. _ Diese Anforderungen bestehen unabhängig davon, ob es sich bei der bezogenen Dienstleistung um eine Haupt- oder ergänzende Nebendienstleistung handelt. _ **9.3** / Keine Änderungen. _ **9.4** / Kommentierung: Die Vereinbarungen, die von der Risikoanalyse aus Kapitel 9.2 betroffen sind, wurden um solche aus dem IT-Betrieb erweitert. Beispielsweise zählen hierzu Informationssicherheitsleit- und -richtlinien). _ Als erforderlich erkannte Maßnahmen sind auch im Fall der Einbindung von Subunternehmen des IT-Dienstleisters zu berücksichtigen. _ **9.5** / Keine Änderungen. _ **9.6** / Kommentierung: Redaktionelle Anpassung des Verweises auf die Nummerierung des aktuellen Dokuments zur VAIT.

10. IT-Notfallmanagement	– **10.1 /** Das IT-Notfallmanagement erhöht die Widerstandsfähigkeit von Bereichen und Prozessen im Unternehmen, um in möglichen Notfallsituationen die Fortführung der Geschäftstätigkeit durch im Vorfeld definierte Verfahren zu gewährleisten. – Dabei werden über die Auswirkungsanalyse (Business Impact Analysis) die zeitkritischen Aktivitäten und Prozesse identifiziert. Zeitkritisch sind grundsätzlich jene Aktivitäten und Prozesse, bei deren Beeinträchtigung für definierte Zeiträume ein nicht mehr akzeptabler Schaden für das Unternehmen zu erwarten ist. – Für die IT-Systeme, welche diese zeitkritischen Aktivitäten und Prozesse unterstützen, werden im Rahmen eines IT-Notfallkonzepts und unter Berücksichtigung der Auswirkungsanalyse und einer Risikoanalyse IT-Notfallpläne erstellt. Diese dokumentieren, wie im Falle eines Notfalls der Normalbetrieb wiederhergestellt und die zeitkritischen Prozesse wieder etabliert werden können. – Im Rahmen des IT-Notfallmanagements ist im Falle einer Ausgliederung auf eine enge Abstimmung mit den Dienstleistern (auch Berücksichtigung von Weiterverlagerung) zu achten. Das IT-Notfallmanagement ist Teil des allgemeinen Notfallmanagements. – **10.2** / Die Geschäftsleitung ist dafür verantwortlich, dass im Rahmen des IT-Notfallmanagements ein IT-Notfallkonzept erstellt wird. Die im IT-Notfallkonzept festgelegten Maßnahmen müssen dazu geeignet sein, das Ausmaß möglicher Schäden zu reduzieren. Das IT-Notfallkonzept ist anlassbezogen zu aktualisieren, regelmäßig auf Aktualität zu überprüfen und angemessen zu kommunizieren. – Im IT-Notfallkonzept werden Verantwortlichkeiten, Ziele und Maßnahmen zur Fortführung bzw. Wiederherstellung von zeitkritischen Aktivitäten und Prozessen bestimmt. Außerdem sind u.a. organisatorische Vorgaben wie z.B. Schnittstellen zu anderen Bereichen (u.a. Risikomanagement oder Informationssicherheitsmanagement) enthalten. – Folgende Szenarien sind mindestens im IT-Notfallkonzept zu berücksichtigen: – (Teil-)Ausfall eines Standortes (z.B. durch Hochwasser, Großbrand, Gebietssperrung, Ausfall der Zutrittskontrolle) – Erheblicher Ausfall von Systemen oder Kommunikationsinfrastruktur (z.B. aufgrund von Fehlern oder Cyberangriffen) – Ausfall einer kritischen Anzahl von Mitarbeitern (z.B. bei Pandemie, Lebensmittvergiftung, Streik) – Ausfall von Dienstleistern (z.B. Zulieferer, Stromversorger) – **10.3 /** Das Unternehmen hat durch eine Auswirkungsanalyse (Business Impact Analysis) die zeitkritischen Prozesse zu identifizieren und für diese die unterstützenden IT-Prozesse, -Systeme, -Ressourcen und weiteren erforderlichen technischen Einrichtungen zu bestimmen. – In Auswirkungsanalysen wird über abgestufte Zeiträume betrachtet, welche Folgen eine Beeinträchtigung von Aktivitäten und Prozessen für den Geschäftsbetrieb haben kann. Die Auswirkungsanalysen sollten u.a. folgende Aspekte berücksichtigen: – Art und Umfang des (im-)materiellen Schadens – Auswirkung des Ausfallzeitpunktes auf den Schaden – **10.4** / Das Unternehmen hat für die identifizierten IT-Prozesse, Systeme, Ressourcen und weiteren erforderlichen technischen Einrichtungen eine Risikoanalyse durchzuführen. In der Risikoanalyse (Risk-Impact-Analysis) werden potentielle Gefährdungen identifiziert und bewertet, welche eine Beeinträchtigung der zeitkritischen Geschäftsprozesse verursachen können. – Die Ergebnisse der Auswirkungsanalyse in Verbindung mit der Risikoanalyse ermöglichen die Entwicklung geeigneter Maßnahmen, um die Aufrechterhaltung der IT-Prozesse, -Systeme, -Ressourcen und weiteren erforderlichen technischen Einrichtungen zu gewährleisten. Die Maßnahmen dienen entweder der Risikoreduzierung oder der Wiederherstellung der Prozesse. – **10.5** / Das Unternehmen hat unter Berücksichtigung der Auswirkungs- und Risikoanalysen für IT-Systeme, welche zeitkritische Aktivitäten und Prozesse unterstützen, IT-Notfallpläne zu erstellen. Hierbei ist das individuelle Risikoprofil zu berücksichtigen. Die IT-Notfallpläne sind angemessen zu kommunizieren und müssen auch im Notfall zugänglich sein. Die IT-Notfallpläne und damit verbundene Dokumente sind regelmäßig und anlassbezogen zu aktualisieren. – IT-Notfallpläne umfassen Wiederanlauf-, Notbetriebs- und Wiederherstellungspläne sowie die dafür festgelegten Parameter und Verantwortlichkeiten und berücksichtigen Abhängigkeiten, um die zeitkritischen Aktivitäten und Prozesse wiederherzustellen. Weiterhin enthalten sie die Bedingungen, die zur Aktivierung der IT-Notfallpläne führen und alle erforderlichen Informationen für eine effektive Kommunikation (unter Berücksichtigung relevanter Dienstleister) im Notfall. – Die Schutzziele sind angemessen zu berücksichtigen. Für den Fall, dass die Wiederherstellung des Normalbetriebs kurzfristig nicht möglich ist (z.B. Pandemie), werden auch alternative Optionen einbezogen. – Parameter umfassen u.a.: – Wiederanlaufzeit (Recovery Time Objective – RTO) – Maximal tolerierbarer Zeitraum, in dem Datenverlust hingenommen werden kann (Recovery-Point-Objective – RPO) – Konfiguration für den Notbetrieb – Abhängigkeiten umfassen u.a.: – Abhängigkeiten von vor- und nachgelagerten Geschäftsprozessen und den eingesetzten IT-Systemen des Unternehmens und der (IT-) Dienstleister – Abhängigkeiten bei der Wiederherstellungspriorisierung der IT-Prozesse und –Systeme – Notwendige Ressourcen, um eine (eingeschränkte) Fortführung der Geschäftsprozesse zu gewährleisten – Abhängigkeiten von externen Faktoren (vorgegeben durch Gesetzgeber, Anteilseigner, Öffentlichkeit, etc.) – **10.6** / Die Wirksamkeit der IT-Notfallpläne ist durch regelmäßige und anlassbezogene Notfalltests zu überprüfen. Die Tests müssen IT-Systeme, welche zeitkritische Aktivitäten und Prozesse unterstützen, vollständig abdecken. Abhängigkeiten zwischen IT-Systemen bzw. von gemeinsam genutzten IT-Systemen sind angemessen zu berücksichtigen. Hierfür ist ein Testkonzept zu erstellen. Die Testergebnisse sind schriftlich zu dokumentieren. Resultierende Mängel sind zu analysieren und an die Geschäftsleitung zu berichten.
	– Das Testkonzept beinhaltet mindestens sowohl Tests einzelner IT-Systeme (z.B. Komponenten, einzelne Anwendungen) als auch deren Zusammenfassung zu Systemverbünden. – **10.7** / Das Unternehmen hat nachzuweisen, dass bei Ausfall eines Rechenzentrums die zeitkritischen Aktivitäten und Prozesse aus einem ausreichend entfernten Rechenzentrum und für eine angemessene Zeit sowie für die anschließende Wiederherstellung des ordentlichen IT-Betriebs erbracht werden können.
11. Kritische Infra-strukturen	– **11.2 – 11.4 /** Kommentierung: Redaktionelle Anpassung des Verweises auf die Nummerierung des aktuellen Dokuments zur VAIT.

3 Auswirkungen für betroffene Institute

Neuregelungen der VAIT betreffen verschiedene Bereiche innerhalb der „Three-Lines-of-Defence“

Durch die Neuregelungen der VAIT resultiert ein **umfassender Handlungsbedarf** für die betroffenen Institute. Dies umfasst insbesondere eine Anpassung der bestehenden IT-Prozesse wie IT-Betrieb inkl. operative Informationssicherheit, Informationsrisikomanagement, Informationssicherheitsmanagement.

Neue VAIT – betroffene Bankbereiche „Three-Lines-of-Defence“

First Line	Second Line	Third Line
• IT-Betrieb (inklusive operative Informationssicherheit)	• Informationsrisikomanagement • Informationssicherheitsmanagement • Risikocontrolling (OpRisk) • Datenschutz	• Interne Revision

Abbildung
Betroffene Bankbereiche durch die Änderungen der VAIT

In Abhängigkeit des Umfangs der Neuregelungen aus den VAIT und dem daraus ableitbaren Handlungsbedarf sollten die Institute im Rahmen von speziellen „Quick-Checks“ die möglichen **Auswirkungen je Anforderungsbereich** einschätzen und die **Betroffenheit je Bereich** indikativ bewerten.

Die Umsetzung der neuen VAIT-Anforderungen ist mit erheblichem Handlungsbedarf verbunden

Vor dem Hintergrund der fehlenden **Umsetzungsfrist** der neuen VAIT ist ein zeitnaher Handlungsbedarf in den einzelnen Instituten erforderlich. Denn die VAIT sind nach Veröffentlichung **sofort** und **ohne weitere Umsetzungsfrist** anzuwenden. Die BaFin begründet das Inkrafttreten ohne Umsetzungsfrist damit, dass grundsätzlich keine neuen Anforderungen für Institute festgelegt würden, sondern lediglich die „übliche Praxis“ niedergeschrieben werde.[1]

Basierend auf den neuen Anforderungen des vorliegenden Rundschreibens der BaFin lassen sich **einzelne Handlungsempfehlungen** (je VAIT-Modul) ableiten:

_ Kapitel 1 – IT-Strategie **HOCH**

- Bei den strategischen Entwicklungen der IT-Aufbau- und Ablauforganisation sind künftig auch wichtige Abhängigkeiten von Dritten (IT-Auslagerungen, sonstiger Fremdbezug von IT-Dienstleistungen) zu berücksichtigen.
- Die Zuordnung der in der IT-Strategie angegebenen gängigen Standards, an denen sich das Institut orientiert, sind auf die Bereiche der Informationssicherheit zu ergänzen.

[1] Vgl. Bankenverband – Schreiben vom 05. März 2021 BdB-Info zu Bankaufsichtliche Anforderungen an die IT, S. 1

- Neben den Zuständigkeiten und der Einbindung der Informationssicherheit in die Organisation sind auch die **Ziele** der **Informationssicherheit** in der IT-Strategie mit aufzunehmen. Dabei sind grundlegende Aussagen zur Schulung und Sensibilisierung zur Informationssicherheit erforderlich. Informationssicherheit muss eigene operationalisierbare Ziele in der Strategie bekommen.
- Das **IT-Notfallmanagement** wird zudem im neuen Kapitel 12 der VAIT präzisiert. Hierbei ist ein klarer Bezug in der IT-Strategie erforderlich.
- Die bisherigen Aussagen zum Notfallmanagement wurden zum IT-Notfallmanagement unter Berücksichtigung der Informationssicherheitsbelange präzisiert.

_ Kapitel 2 – IT-Governance Gering

- Die Forderung nach einer höheren **Ressourcenausstattung** im Bereich des Informationsrisikomanagements, des Informationssicherheitsmanagements, dem IT-Betrieb und der Anwendungsentwicklung wurde neben der quantitativ und qualitativ angemessenen Personalausstattung um die Ressourcenausstattung erweitert.
- Hinsichtlich der Maßnahmen zur Erhaltung einer angemessenen qualitativen Ressourcenausstattung sind (**personelle, finanzielle und sonstige Ressourcen**) erforderlich, die insbesondere den Stand der Technik sowie die aktuelle und zukünftige Bedrohungslage berücksichtigen.

_ Kapitel 3 - Informationsrisikomanagement HOCH

- Innerhalb der IT-Risikokriterien, die die Grundlage für diverse Identifikations-, Bewertungs-, Überwachsungs- und Steuerungsprozesse darstellen, sollen nun auch die Kritikalität der Geschäftsprozesse und -aktivitäten sowie bekannte Gefährdungen und Vorfälle aus der Vergangenheit berücksichtigt werden (incl. Cyberrisiken und abgeleitete Maßnahmen zur Prävention).
- Innerhalb der Erfassung des Informationsrisikomanagements ist der Informationsverbund zu erweitern. Dieser soll um geschäftsrelevante Informationen, Geschäfts- und Unterstützungsprozesse, IT-Systeme und die zugehörigen IT-Prozesse sowie Netz- und Gebäudeinfrastrukturen ergänzt werden.
- Weitere Ergänzungen beinhalten Abhängigkeiten und Schnittstellen in Bezug auf die Vernetzung des Informationsverbundes mit Dritten, die künftig noch stärker berücksichtigt werden müssen.
- Das Institut hat sowohl regelmäßig als auch anlassbezogen den Schutzbedarf für die Bestandteile seines definierten Informationsverbundes, insbesondere im Hinblick auf die Schutzziele „Integrität“, „Verfügbarkeit“, „Vertraulichkeit“ und „Authentizität“ zu ermitteln (Überarbeitungsintervall des Schutzbedarfs).
- Es ist künftig neu zu regeln, dass der Eigentümer der Information die Ermittlung des Schutzbedarfs verantwortet (Verantwortlichkeit, Kompetenz).
- Die Schutzbedarfsfeststellung sowie die zugehörige Dokumentation sind durch das Informationsrisikomanagement (Second-Line-of-Defence) zu überprüfen.
- Das Institut hat Anforderungen zu definieren, die zur Erreichung des jeweiligen Schutzbedarfs angemessenen sind und in geeigneter Form dokumentiert werden (**Sollmaßnahmenkatalog**).
- Das Institut hat auf Basis der festgelegten Risikokriterien regelmäßig eine Risikoanalyse durchzuführen. Diese Analyse ist zu koordinieren und zu dokumentieren. Die

Risikoanalyse erfolgt auf Grundlage eines Vergleichs der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen (Soll-Ist-Vergleich).

- Die Risikoanalyse hat über den Soll-Ist-Vergleich hinaus u.a. mögliche Bedrohungen, das Schadenspotenzial, die Schadenshäufigkeit sowie den Risikoappetit zu berücksichtigen.
- Weiterhin sind hierbei **sonstige risikoreduzierende Maßnahmen** zu berücksichtigen.
- Wenn Sollmaßnahmen nicht implementiert werden können (z.B. wegen technischer Restriktionen), sollen künftig sonstige risikoreduzierende Maßnahmen umgesetzt werden.
- Die Behandlung der IT-Risiken ist **kompetenzgerecht** zu dokumentieren (Nachweis ist auch für in- und externe Prüfungen notwendig).
- Das Institut hat sich laufend über Bedrohungen seines Informationsverbundes zu informieren, die Relevanz zu prüfen, die Auswirkung zu bewerten und sofern erforderlich, geeignete technische und organisatorische Maßnahmen zu ergreifen.
- Hierbei sind auch interne und externe Veränderungen (z.B. der **Bedrohungslage**) zu berücksichtigen.
- Mögliche Maßnahmen können z.B. die direkte Warnung von Mitarbeitern, das Sperren von betroffenen Schnittstellen und den Austausch von betroffenen IT-Systemen umfassen.
- Die **Bedrohungen** müssen in Form eines schlüssigen Konzepts analysiert werden.
- In der regelmäßigen (mindestens jedoch jährlichen oder ggf. ad hoc) Berichterstattung der Ergebnisse der Risikoanalyse an die Geschäftsleitung sind künftig bei Berücksichtigung der Risikosituation auch externe potenzielle Bedrohungen mit aufzuführen.

_ Kapitel 4 – Informationssicherheitsmangement HOCH

- Die Informationssicherheitsleitlinie ist künftig bei wesentlichen Veränderungen der Rahmenbedingungen zu prüfen und bei Bedarf zeitnah anzupassen (Eine Anpassung ist in der Praxis beispielsweise bei Änderung der Bedrohungslage erforderlich).
- In der Informationssicherheitsleitlinie werden die Eckpunkte zum Schutz von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität sowie der Geltungsbereich für die Informationssicherheit festgelegt.
- Darüber hinaus werden die wesentlichen organisatorischen Aspekte sowie die wichtigsten Rollen und Verantwortlichkeiten des Informationssicherheitsmanagements beschrieben.
- Mit der Leitlinie soll die Geschäftsleitung u.a. folgende neu eingeführte Kriterien darlegen:
  - ihre Gesamtverantwortung für die Informationssicherheit
  - Frequenz und Umfang des Berichtswesens zur Informationssicherheit
  - die Kompetenzen im Umgang mit Informationssicherheitsrisiken
  - die grundlegenden Anforderungen der Informationssicherheit an Personal, Auftragnehmer, Prozesse und Technologien
  - geeignete Kriterien für die Information der Geschäftsleitung über Informationssicherheitsvorfälle sofern diese Kriterien nicht in einer Informationssicherheitsleitlinie dargelegt werden.
- Rahmenbedingungen umfassen u.a. interne Veränderungen der IT-Aufbau- und IT-Ablauforganisation oder der IT-Systeme des Instituts sowie äußere Veränderungen (z.B. Bedrohungsszenarien) oder rechtliche Anforderungen.
- In den Informationssicherheitsrichtlinien sind die Ergänzungen bezüglich des **Identitäts- und Rechtemanagements** sowie des **Perimeter- und Gebäudeschutzes** neu aufzunehmen.

- Das Institut hat eine Richtlinie über das Testen und Überprüfen der Maßnahmen zum Schutz der Informationssicherheit einzuführen und diese **regelmäßig und anlassbezogen** zu überprüfen und bei Bedarf anzupassen. Die ausreichende Qualifikation der Tester ist zu gewährleisten.
- Die Richtlinie berücksichtigt u.a.:
  - die allgemeine Bedrohungslage
  - die individuelle Risikosituation des Unternehmens
  - Kategorien von Test- und Überprüfungsobjekten (z.B. das Unternehmen, IT-Systeme, Komponenten)
  - Art, Umfang und Frequenz von Tests und Überprüfungen
  - Zuständigkeiten und Regelungen zur Vermeidung von Interessenkonflikten.
- Künftig ist es die originäre Aufgabe der Geschäftsleitung, die Funktion des Informationssicherheitsbeauftragten inkl. Stellvertretung einzurichten.
- Weiterhin sind die Aufgaben der Funktion des Informationssicherheitsbeauftragten in den Stellen- und Funktionsbeschreibungen im Hinblick auf die folgenden Punkte zu ergänzen:
  - IT- und Informationssicherheitsbelange sind künftig auch bei der Erstellung und Fortschreibung des Notfallkonzepts durch den Informationssicherheitsbeauftragten anzumerken.
  - Der Informationssicherheitsbeauftragte hat zudem die neue Aufgabe, auf die Überwachung und Hinwirkung der Einhaltung der Informationssicherheit bei Projekten und Beschaffungen hinzuwirken.
  - Der Informationssicherheitsbeauftragte kann durch ein Informationssicherheits-management-Team unterstützt werden.
- In der Aufbau- und Ablauforganisation ist die Funktion des Informationssicherheitsbeauftragten angemessen unabhängig zu gestalten, um mögliche Interessenkonflikte zu vermeiden.
- Um dies gewährleisten zu können, sind ein Vertreter und ggf. weitere Stellen zu benennen. Für den Informationssicherheitsbeauftragten, seinen Vertreter und ggf. weitere Stellen sind Funktions- und Stellenbeschreibungen zu erstellen sowie Budgets zuzuweisen.
- Nach einem **Informationssicherheitsvorfall** sind die Auswirkungen auf die Informationssicherheit **zeitnah** zu **analysieren** und angemessene Nachsorgemaßnahmen zu veranlassen.
- Die Definition des Begriffes „**Informationssicherheitsvorfall**“ ist zu überarbeiten. Danach orientieren sich Art und Umfang am Schutzbedarf der betroffenen Bestandteile des Informationsverbundes. Ein Informationssicherheitsvorfall kann auch dann vorliegen, wenn mindestens **eines** der Schutzziele („Verfügbarkeit“, „Integrität“, „Vertraulichkeit“, „Authentizität“) gemäß den Vorgaben des institutsspezifischen Sollkonzepts der Informationssicherheit verletzt ist.
- Die Begriffe „**Informationssicherheitsvorfall**“, „**sicherheitsrelevantes Ereignis**“ (im Sinne der operativen IT-Sicherheit) und „Abweichung vom Regelbetrieb“ (im Sinne von „Störung im Tagesbetrieb“) sollen in den Arbeitsanweisungen nachvollziehbar voneinander abgegrenzt werden.
- Das Institut hat ein kontinuierliches und angemessenes **Sensibiliseriungs- und Schulungsprogramm** für Informationssicherheit festzulegen.

- Der **Erfolg** der festgelegten **Sensibilisierungs- und Schulungsmaßnahmen** ist durch das Institut zu überprüfen.
- Das Programm sollte **mindestens** folgende Aspekte berücksichtigen:
  - Persönliche Verantwortung für eigene Handlungen und Unterlassungen sowie allgemeine Verantwortlichkeiten zum Schutz von Informationen und
  - grundsätzliche Verfahren zur Informationssicherheit (wie Berichterstattung über Informationssicherheitsvorfälle) und allgemeingültige Sicherheitsmaßnahmen (z.B. zu Passwörtern, Social Engineering, Prävention vor Schadsoftware und dem Verhalten bei Verdacht auf Schadsoftware).

Kapitel. 5 – Operative Informationssicherheit HOCH

- Das Institut hat auf Basis der Informationssicherheitsleitlinie und Informationssicherheits-richtlinien angemessene, dem Stand der Technik entsprechende, **operative Informationssicherheitsmaßnahmen** und **Prozesse** zu implementieren.
- Die **Informationssicherheitsmaßnahmen** und **-prozesse** haben u.a. folgende Inhalte zu berücksichtigen:
  - Schwachstellenmanagement zur Erkennung, Bewertung, Behandlung und Dokumentation von Schwachstellen
  - Segmentierung und Kontrolle des Netzwerks (einschließlich Richtlinienkonformität der Endgeräte)
  - Sichere Konfiguration von IT-Systemen (Härtung)
  - Verschlüsselung von Daten bei Speicherung und Übertragung gemäß Schutzbedarf
  - mehrstufiger Schutz der IT-Systeme gemäß Schutzbedarf (z.B. vor Datenverlust, Manipulation oder Verfügbarkeitsangriffen oder vor nicht autorisiertem Zugriff)
  - Perimeterschutz von z.B. Liegenschaften, Rechenzentren und anderen sensiblen Bereichen

- Künftig sind die **Gefährdungen** des **Informationsverbundes** möglichst **frühzeitig** zu **identifizieren – hierbei ist die Einführung von SIEM-Systemen sinnvoll**.
- Potentiell **sicherheitsrelevante Informationen** sind angemessen, zeitnah, regelbasiert und zentral auszuwerten.
- Diese Informationen müssen bei Transport und Speicherung geschützt werden und für eine angemessene Zeit zur späteren Auswertung zur Verfügung stehen.
- Es ist ein angemessenes **Portfolio** an **Regeln** zur **Identifizierung sicherheitsrelevanter Ereignisse** zu definieren.
- Die Regeln sind vor Inbetriebnahme zu testen.
- Die Regeln sind regelmäßig und anlassbezogen auf Wirksamkeit zu prüfen und weiterzuentwickeln.
- Künftig sind auch **sicherheitsrelevante Ereignisse** zeitnah zu analysieren und auf daraus resultierenden Informationssichervorfällen ist unter Koordination des Informationssicherheitsmanagements angemessen zu reagieren.
- Künftig ist die **Sicherheit** der **IT-Systeme** regelmäßig, anlassbezogen und unter Vermeidung von Interessenkonflikten zu überprüfen.
- Ergebnisse sind hinsichtlich notwendiger Verbesserungen zu analysieren und Risiken angemessen zu steuern.

- Turnus, Art und Umfang der Überprüfung sollten sich insbesondere **am Schutzbedarf** und der **potentiellen Angriffsfläche** (z.B. Erreichbarkeit aus dem Internet) des IT-Systems orientieren.
- **Arten** der **Überprüfungen** sind zu definieren wie z.B.: Abweichungsanalysen (Gap-Analysen), Schwachstellenscans, Penetrationstests und Simulationen von Angriffen.

_ Kapitel 6 – Identitäts- und Rechtemanagement HOCH

- Die Inhalte der Berechtigungskonzepte wie Umfang und Nutzungsbedingungen der Berechtigungen, sind um Zugang zu IT-Systemen, Datenzugriff sowie um Zutrittsrechte zu Räumen zu erweitern.
- Diese sind konsistent zum ermittelten Schutzbedarf sowie vollständig und nachvollziehbar ableitbar für alle bereitgestellten Berechtigungen festzulegen.
- Im Grundsatz Berechtigungskonzepte ist der Sparsamkeitsgrundsatz „**Need-to-Know**“ um den Grundsatz „**Least-Privilege**“ zu erweitern.
- Die Funktionstrennung ist künftig auch berechtigungskonzeptübergreifend zu wahren und **Interessenkonflikte** sind zu **vermeiden**. Dies ist zu regeln.
- Berechtigungskonzepte sind **regelmäßig** und **anlassbezogen** zu **überprüfen** und ggf. zu aktualisieren.
- Folgende Erläuterungen sind in den Anweisungen der Berechtigungskonzepte zu berücksichtigen:
  - Technische Benutzer sind z.B. Benutzer, die von IT-Systemen verwendet werden, um sich gegenüber anderen IT-Systemen zu identifizieren oder um eigenständig IT-Routinen auszuführen.
  - Zugangs- und Zugriffsberechtigungen auf IT-Systeme können auf allen Ebenen eines IT-Systems (z.B. Betriebssystem, Datenbank, Anwendung) vorliegen.
- Im Rahmen des Sparsamkeitsgrundsatzes sind nicht benötigte Benutzerzugänge zu löschen
- Künftig müssen **Zugriffe** und **Zugänge** jederzeit zweifelsfrei einer handelnden bzw. **verantwortlichen Person** (möglichst automatisiert) zugeordnet werden. Dies ist zu regeln.
- Das Institut muss regeln, dass **automatisierte Aktivitäten** den verantwortlichen Personen zuzuordnen sind.
- Es ist zu regeln, dass **Abweichungen** in begründeten Ausnahmefällen und die hieraus resultierenden Risiken zu bewerten, zu dokumentieren und anschließend von der fachlich verantwortlichen Stelle zu genehmigen sind.
- Die Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen ist künftig zeitnah oder unverzüglich vorzunehmen.
- Bei den Gründen für eine **unverzügliche Deaktivierung** bzw. **Löschung** von Berechtigungen ist u.a. die Gefahr einer missbräuchlichen Verwendung (z.B. bei fristloser Kündigung eines Mitarbeiters) in den Anweisungen mit aufzunehmen.
- Das Institut hat nach Maßgabe des Schutzbedarfs und der Soll-Anforderungen **Prozesse** zur **Protokollierung** und **Überwachung** einzurichten, die überprüfbar machen, dass die Berechtigungen nur wie vorgesehen eingesetzt werden.
- Das Institut hat insbesondere für die Aktivitäten mit **privilegierten** (besonders kritischen) **Benutzer**- und **Zutrittsrechten** angemessene Prozesse zur Protokollierung und Überwachung einzurichten.

- Berechtigungen sind generell **risikoorientiert** gesondert zu überwachen.
- Die **übergeordnete Verantwortung** für die Prozesse zur Protokollierung und Überwachung von Berechtigungen ist einer Stelle zuzuordnen, die unabhängig vom berechtigten Benutzer oder dessen Organisationseinheit ist.
- Zu **privilegierten Zutrittsrechten** sind künftig die Rechte zum Zutritt zu Rechenzentren, Technikräumen sowie sonstigen sensiblen Bereichen hinzuzuzählen.

_Kapitel 7. IT-Projekte und Anwendungsentwicklung HOCH

- Die **organisatorischen Grundlagen** für **IT-Projekte** sind neu zu priorisieren bzw. zu ergänzen. Notwendig ist künftig die Einbindung betroffener Beteiligter (insbesondere des Informationssicherheitsbeauftragten), Projektdokumentation (z.B. Projektantrag, Projektabschlussbericht), quantitative und qualitative Ressourcenausstattung, Steuerung der Projektrisiken, Informationssicherheitsanforderungen, projektunabhängige Qualitätssicherungsmaßnahmen und Aufarbeitung der gewonnenen Erkenntnisse (Lessons Learned).
- Künftig müssen im Rahmen von IT-Projekten **größere Änderungen** an Prozessen mit Auswirkungen auf die Informationssicherheit, durch entsprechende Änderungsanträge genehmigt werden.
- Für Anforderungen an die Funktionalität der Anwendnung wie auch nichtfunktionale Anforderungen müssen entsprechende **Akzeptanz- und Testkriterien** definiert werden.
- Künftig ist zur Sicherstellung der Integrität der Anwendungsentwicklung beispielsweise eine Versionierung des **Quellcodes** und der **Anforderungsdokumente** zu dokumentieren (Revisionstechnisch lückenlose Dokumentation).
- Künftig haben die Tests in ihrem Umfang die Funktionalität der Anwendung, die implementierten Maßnahmen zum Schutz der Informationen und bei Relevanz die Systemleistung unter verschiedenen **Stressbelastungsszenarien** mit einzubeziehen.
- Die fachlich zuständigen Stellen haben die Durchführung von Abnahmetests zu verantworten.
- Testumgebungen zur **Durchführung** der **Abnahmetests** haben in für den Test wesentlichen Aspekten der Produktionsumgebung zu entsprechen.
- Die **Testaktivitäten** und **Testergebnisse** sind zu dokumentieren.
- Die **Testdurchführung** erfordert eine einschlägige Expertise der Tester sowie eine angemessen ausgestaltete Unabhängigkeit von den Anwendungsentwicklern.
- Der Schutzbedarf der zum Test verwendeten Daten ist dabei zu berücksichtigen.
- Risikoorientiert schließen die Maßnahmen zum Schutz der Informationen auch Penetrationstests ein.

- Die Anforderungen des Testens gelten prinzipiell auch für die individuelle Datenverarbeitung **(IDV)**.

_Kapitel 8 IT-Betrieb HOCH

- Die bisherige Anforderung, die Komponenten der IT-Systeme und deren Beziehungen zueinander in geeigneter Weise zu verwalten, ist um die erfassten Bestandsangaben regelmäßig sowie anlassbezogen zu aktualisieren.

- Die aufsichtlich geforderte Ergänzung des Inventars erfordert künftig die Information über den Eigentümer sowie den Schutzbedarf der IT-Systeme und ergänzt die bisherigen Informationen.
- Das **Portfolio** aus **IT-Systemen** bedarf der Steuerung durch die Institute.
- IT-Systeme sollten regelmäßig aktualisiert werden.
- Risiken aus veralteten bzw. nicht mehr vom Hersteller unterstützten IT-Systemen sind zu berücksichtigen (**Lebenszyklus-Management**).
- Nicht mehr verwendete Hardwarekomponenten sind sicher zu entsorgen.
- Änderungen von IT-Systemen und größeren Prozessänderungen mit **Auswirkungen auf die Informationssicherheit** sind zu beantragen. Die Anträge sind in **geordneter Art und Weise** aufzunehmen, zu dokumentieren, zu bewerten, zu priorisieren und zu genehmigen.
- Für zeitkritische Änderungen von IT-Systemen sind geeignete Prozesse einzurichten.
- Die Meldungen über ungeplante Abweichungen vom Regelbetrieb (**Störungen**) und deren Ursachen wurden um neue Ergänzungen modifiziert.
- Standardvorgehensweisen z.B. für Maßnahmen und Kommunikation sowie Zuständigkeiten (z.B. für Informationssicherheitsvorfälle, Fehlfunktionen) sind zu definieren.
- Das Institut hat bei den geeigneten Kriterien für die Information der Beteiligten künftig neben der Geschäftsleitung auch die **zuständige Aufsichtsbehörde** als Adressat über Störungen festzulegen.
- Der aktuelle **Leistungs-** und **Kapazitätsbedarf** der IT-Systeme ist zu erheben und der zukünftige Leistungs- und Kapazitätsbedarf ist abzuschätzen.
- Die **Leistungserbringung** ist zu planen und zu überwachen, um insbesondere Engpässe zeitnah zu erkennen und angemessen zu reagieren.
- Bei der Planung ist der Leistungs- und Kapazitätsbedarf von Informations-sicherheitsanforderungen zu berücksichtigen.

_ Kapitel 9 Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen **Gering**

- Das Institut hat in Bezug auf jede sonstige Dienstleistungsbeziehung im Bereich der IT-Dienstleistungen vorab eine Erhebung und Bewertung von **funktionalen** und **nicht funktionalen Anforderungen** sowie eine Risikoanalyse durchzuführen.
- Die aus der Risikobewertung zum sonstigen Fremdbezug von IT-Dienstleistungen abgeleiteten Maßnahmen (wie z.B. Einholung von Reports etc.) sind in der **Vertragsgestaltung** zu berücksichtigen.
- Künftig beinhaltet dies beispielsweise auch mögliche Vereinbarungen zum Informationsrisikomanagement, zum Informationssicherheitsmanagement, zum Notfallmanagement und IT-Betrieb, die im Regelfall den Zielvorgaben des Instituts entsprechen.

_ Kapitel 10 IT-Notfallmanagement **HOCH**

- Die **Geschäftsleitung** hat Ziele zum IT-Notfallmanagement zu definieren und hieraus abgeleitet einen Notfallmanagementprozess festzulegen.
- Die im Notfallkonzept festgelegten Maßnahmen müssen dazu geeignet sein, das Ausmaß möglicher Schäden zu **reduzieren** (vgl. AT 7.3 Tz. 1 MaRisk).

- Die **Wirksamkeit** und **Angemessenheit** des Notfallkonzeptes ist regelmäßig zu überprüfen.
- Für Notfälle in zeitkritischen Aktivitäten und Prozessen ist Vorsorge zu treffen (Notfallkonzept).
- Das Notfallkonzept muss **Geschäftsfortführungs-** sowie **Wiederherstellungspläne** umfassen.
- Im Fall der Auslagerung von zeitkritischen Aktivitäten und Prozessen haben das auslagernde Institut und das Auslagerungsunternehmen über aufeinander **abgestimmte Notfallkonzepte** zu verfügen (vgl. AT 7.3 Tz. 2 MaRisk).
- Für **zeitkritische Aktivitäten** und **Prozesse** sind die Notfallkonzepte für alle relevanten Szenarien mindestens jährlich und anlassbezogen nachzuweisen (vgl. AT 7.3 Tz. 3 MaRisk).
- Die **Ziele** und **Rahmenbedingungen** des IT-Notfallmanagements sind auf Basis der Ziele des Notfallmanagements festzulegen.
- Die **Rahmenbedingungen** müssen u.a. organisatorische Aspekte wie z.B. Schnittstellen zu anderen Bereichen (u.a. Risikomanagement oder Informationssicherheitsmanagement) enthalten.
- Das Institut hat auf Basis des Notfallkonzepts für alle IT-Systeme, welche zeitkritische Aktivitäten und Prozesse unterstützen, **IT-Notfallpläne** zu erstellen.
- Diese **IT-Notfallpläne** haben Wiederanlauf-, Notbetriebs- und Wiederherstellungspläne sowie die dafür festgelegten Parameter und berücksichtigten Abhängigkeiten zu enthalten, um die zeitkritischen Aktivitäten und Prozesse wiederherzustellen.
- Die Parameter der IT-Notfallpläne haben **folgende Mindestangaben** zu umfassen, u.a.:
  - Wiederanlaufzeit (Recovery Time Objective – RTO)
  - Maximal tolerierbarer Zeitraum, in welchem ein Datenverlust hingenommen werden kann (Recovery Point Objective – RPO)
  - Konfiguration für den Notbetrieb
- Die künftige Prüfung der **Abhängigkeiten** der **IT-Notfallpläne** umfasst folgende Kriterien:
  - Abhängigkeiten von vor- und nachgelagerten Geschäftsprozessen und den eingesetzten IT-Systemen des Instituts und der (IT-) Dienstleister
  - Abhängigkeiten bei der Wiederherstellungspriorisierung der IT-Prozesse und -Systeme
  - Notwendige Ressourcen, um eine (eingeschränkte) Fortführung der Geschäftsprozesse zu gewährleisten
  - Abhängigkeiten von externen Faktoren (Gesetzgeber, Anteilseigner, Öffentlichkeit, etc.).
- Auch in den neuen VAIT ist die Wirksamkeit der IT-Notfallpläne durch **regelmäßige und anlassbezogene Notfalltests** zu überprüfen.
- Die Tests müssen alle IT-Systeme, welche **zeitkritische Aktivitäten** und **Prozesse** unterstützen, vollständig **abdecken**.
- **Abhängigkeiten** zwischen **IT-Systemen** bzw. von gemeinsam genutzten IT-Systemen sind angemessen zu berücksichtigen; hierfür ist ein Testkonzept zu erstellen.
- Das **IT-Testkonzept** hat sowohl Tests einzelner IT-Systeme (z.B. Komponenten, einzelne Anwendungen) als auch deren Zusammenfassung zu Systemverbünden (z.B.

Hochverfügbarkeitscluster) sowie Prozesse (z.B. Zutritts- und Zugriffsmanagement) zu beinhalten.

- Das Institut hat nachzuweisen, dass bei Ausfall eines Rechenzentrums die zeitkritischen Aktivitäten und Prozesse aus einem ausreichend entfernten Rechenzentrum (Ersatzrechenzentrum) und für eine angemessene Zeit sowie für die anschließende Wiederherstellung des IT-Normalbetriebs erbracht werden können.

_ Kapitel 11 – Kritische Infrastrukturen - Ohne

- Keine inhaltlichen Neuerungen, daher auch kein Handlungsbedarf

4 Unser Lösungsansatz – VAIT Quick-Check

Der **VAIT Quick-Check** stellt einen strukturierten Ansatz dar, um schnell und zuverlässig einen transparenten Überblick über den erforderlichen Anpassungsbedarf der internen Risikomanagementsysteme und -verfahren zu erhalten.

Grundlage des **VAIT Quick-Check** ist eine praxiserprobte Vorgehensweise, welche anhand der neuen VAIT-Anforderungen den Erfüllungsgrad bewertet und den **notwendigen (Mindest-)Anpassungs- und Optimierungsbedarf im Risikomanagement** frühzeitig definiert.

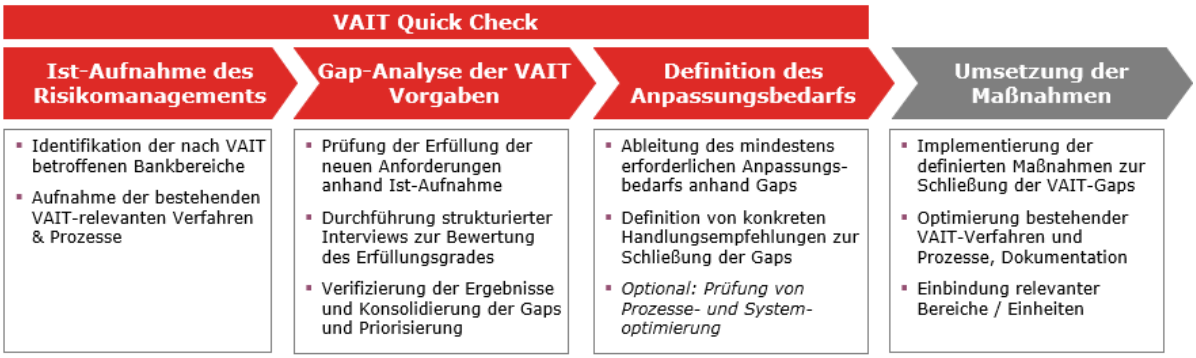

Abbildung
VAIT Quick- Check im Überblick

Der **VAIT Quick-Check** bietet einen fundierten Lösungsansatz für Kreditinstitute, um zuverlässig einen **vollständigen Überblick über die Erfüllung der VAIT-Vorgaben** zu erhalten – ressourcenschonend und effektiv. Der Quick-Check ist skalierbar auf die jeweilige Institutsgröße und ermöglicht eine **strukturierte Erfassung des Handlungsbedarfs je nach betroffenem Organisationsbereich**.

5 Ihr Nutzen - Vorteile durch bewährten Ansatz

Wir unterstützen Sie mit bewährten Ansätzen und ausgeprägter Expertise im Risikomanagement von Banken - **ressourcenschonend und zuverlässig -** bei der Weiterentwicklung der versicherungsaufsichtlichen Anforderungen an die IT.

Der bewährte **VAIT Quick-Check** bietet für Institute zahlreiche Vorteile:

- ✓ Transparenz über den **Erfüllungsgrad der Vorgaben** der VAIT-Novelle und über die **betroffenen Bankbereiche**
- ✓ Identifikation von **prozessualen Schwachstellen und Verfahrenslücken** im bestehenden Risikomanagement und dessen bisheriger Umsetzung
- ✓ Effizienzgewinn und Ressourcenschonung durch eine **strukturierte Vorgehensweise**
- ✓ Kombination von fachlicher **IT-Management-Expertise** und methodischer **Projekterfahrung**
- ✓ Einbringen von Erkenntnissen aus einer Vielzahl von Projekten aus IT-Management und IT-Risikokontrollumfeld (**„Best Practice-Standards"**)
- ✓ Prüfungskonforme Bewertung regulatorischer Vorgaben (optional: Zertifizierung der Ergebnisse durch Wirtschaftsprüfer möglich)

Der konventionelle Umgang mit regulatorischen Anforderungen ist häufig ineffektiv und basiert auf einer isolierten Betrachtung oder mangelnder Transparenz. Um Ineffizienzen zu beheben und Redundanzen abzubauen, bieten Severn und ORO Lösungsansätze wie das „**Outsourced Regulatory Office**" (www.regupedia.de) oder „**integrierte Risikomanagement-Systeme**" an. Durch praxiserprobte Lösungen werden nachweislich Synergiepotenziale identifiziert, operative Prozesse optimiert und letztlich Effizienzgewinne realisiert.

6 Severn Consultancy und ORO Services – Ihre Partner im Risikomanagement

Profitieren Sie von unserer langjährigen Expertise im Risiko- und Compliance-Management

Die Berater von Severn und ORO verfügen über **langjährige Erfahrungen in der Umsetzung von aufsichtsrechtlichen Anforderungen** für Versicherungen und Banken. Ferner können wir auf fundierte fachliche und methodische Expertise in der Analyse von Prozessen im Risikomanagement sowie in der Etablierung risikoorientierter Managementverfahren zurückgreifen.

Eine Vielzahl erfolgreich durchgeführter Projekte **im Bereich der versicherungs- und bankaufsichtlichen Anforderungen an die IT** für **internationale Versicherungen, Großbanken** sowie **führende Privatbanken** und **Asset Manager** bestätigen die langjährige vertrauensvolle Zusammenarbeit mit unseren Kunden.

Projekterfahrungen (Auszug):

_ **Internationales Zahlungs- und E-Geld-Institut:** Testbetrieb des ZAIT-Tools mit „Just-In-Time Servicing" der Ergebnisse.

_ **Internationale Tochter einer Großbank:** BAIT-Quick-Check mit Einsatz des BAIT-Tools zur GAP-Analyse. Anschließendes Umsetzungsprojekt der BAIT.

_ **Internationale Börse:** Umsetzung der regulatorischen Anforderungen im Bereich der IT. Gesamtkoordination der Umsetzungserfahrungen und Berichterstattung an GL und Aufsichtsorgan.

_ **Genossenschaftsbank:** Unterstützung bei der Umsetzung der Anforderungen an die bankaufsichtlichen Erfordernisse an die BAIT. Erstellung eines Lastenheftes im Bereich des IT-Störungsmanagements.

_ **Nationale Versicherung:** Unterstützung bei der Umsetzung der Anforderungen an die individuelle Datenverarbeitung (IDV) als Teilbereich der BAIT.

_ **Internationale Großbank:** Durchführung eines BAIT-Quick-Checks. Unterstützung bei der Umsetzung der Anforderungen an die bankaufsichtlichen Erfordernisse an die BAIT. Erstellung eines Lastenheftes im Bereich des IT-Störungsmanagements.

_ **Lokale Privatbank:** Testbetrieb des BAIT-Tools mit „Just-In-Time Servicing" der Ergebnisse.

7 Next Generation Consulting für Finanzunternehmen

Severn Consultancy (www.severn.de) ist eine auf den nationalen und internationalen Finanzmarkt spezialisierte Unternehmensberatung. Unsere besondere Expertise liegt in der effektiven Realisierung erfolgskritischer Veränderungsprozesse – dort sind wir besser als viele andere.

In mehr als 25 Jahren Beratungspraxis haben wir eine Vielzahl renommierter Banken und Finanzdienstleister bei der effizienten Durchführung ihrer Projekte und der Optimierung unternehmensinterner Prozesse unterstützt.

Kompetente Fach- und Managementberatung gepaart mit effektivem Projekt-Management, wirkungsvoller Organisationsentwicklung und zukunftssicherem IT-Management sind die Säulen des „Severn way to get it done".

Über unsere Tochtergesellschaft ORO Services GmbH („Outsourced Regulatory Office") bieten wir mit dem Kernprodukt Regupedia® (www.regupedia.de) ein umfassendes Informationsportal zur Finanzmarktregulierung.

Unsere Mandanten schätzen unsere innovativen Beratungskonzepte, das methodische Know-how sowie unsere fundierten Markt- und Branchenkenntnisse. Die meisten unserer Mandanten unterstützen wir bereits seit vielen Jahren in einer vertrauensvollen Zusammenarbeit.

Ansprechpartner

Axel Becker | Senior Manager bei ORO Services

Marius Tippmann | Senior Consultant bei ORO Services

Severn Consultancy GmbH | ORO Services GmbH
Hansa Haus, Berner Straße 74
60437 Frankfurt am Main
T +49 (0)69 / 950 900-0
F +49 (0)69 / 950 900-50

info@severn.de | redaktion@oro-services.de
www.severn.de | www.oro-services.de | www.regupedia.de

Axel Becker
Senior Manager /
ORO Services GmbH

Marius Tippmann
Senior Consultant /
ORO Services GmbH