BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

Rundschreiben 10/2018 (VA) in der Fassung vom ~~XX.XX.2021~~03.03.2022

Versicherungsaufsichtliche Anforderungen an die IT (VAIT)

Inhalt

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

I. Vorbemerkung

1 Der Einsatz von Informationstechnik (IT) in den Unternehmen, auch unter Einbeziehung von IT-Services, die durch IT-Dienstleister bereitgestellt werden, hat eine zentrale Bedeutung für Versicherungsunternehmen und Pensionsfonds. Dieses Rundschreiben enthält Hinweise zur Auslegung der Vorschriften über die Geschäftsorganisation im Versicherungsaufsichtsgesetz (VAG), soweit sie sich auf die technisch-organisatorische Ausstattung der Unternehmen beziehen. Es legt diese Vorschriften für die BaFin verbindlich aus und gewährleistet hierdurch eine konsistente Anwendung gegenüber allen Unternehmen und Gruppen. Das Rundschreiben gibt einen flexiblen und praxisnahen Rahmen vor, insbesondere für das Management der IT-Ressourcen, für das Informationsrisikomanagement und das Informationssicherheitsmanagement.

2 Dieses Rundschreiben findet Anwendung auf 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.

3 Das Rundschreiben betrifft Gruppen, wenn alle gruppenzugehörigen Erst- und Rückversicherungsunternehmen ihren Sitz im Inland haben. Es betrifft außerdem 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.

4 Für Unternehmen, die ~~dem Anwendungsbereich des Aufsichtssystems Solvabilität II unterliegen, bleiben die in den~~ 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.

5 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.

~~5~~6 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 ~~der internationale Sicherheitsstandard~~die internationalen Sicherheitsstandards ISO/IEC ~~2700X~~270XX der International Organization for Standardization.

~~6~~7 Bei der Umsetzung der Anforderungen an die Geschäftsorganisation und somit auch der Ausgestaltung der Strukturen, IT-Systeme oder Prozesse spielt das Proportionalitätsprinzip eine erhebliche Rolle. 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~~).~~)[1]. Das Proportionalitätsprinzip knüpft also an das individuelle Risikoprofil eines jeden Unternehmens an. Geringe Größe kann ein Indikator für ein schwächer ausgeprägtes Risikoprofil sein - und umgekehrt. Soweit die Mitarbeiterzahl bei der Bestimmung der Größe eine Rolle spielen kann, ist nicht auf die vorhandenen Mitarbeiter abzustellen, sondern auf den tatsächlichen Mitarbeiterbedarf. Das heißt vor allem, dass auch Mitarbeiterkapazitäten, die das Unternehmen im Wege der Ausgliederung heranzieht, in die Betrachtung einzubeziehen sind.

~~7~~8 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.

~~8~~9 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.

~~9~~10 Die Fragen, welche konkreten Strukturen, IT-Systeme oder Prozesse einem bestimmten Risikoprofil angemessen sind sowie ob und ggf. welche begleitenden Maßnahmen erforderlich sind, können nur im jeweiligen Kontext (unter Berücksichtigung u. a. der Kritikalität) beantwortet werden.

11 Die vom Unternehmen getroffene Feststellung des individuellen Risikoprofils wirkt fort, sofern sich keine Veränderungen ergeben haben.

[1] Für Einrichtungen der betrieblichen Altersversorgung (EbAV) sind die Anforderungen so umsetzen, dass der Größenordnung, der Art, dem Umfang und der Komplexität ihrer Tätigkeiten Rechnung getragen wird (s. § 296 Abs. 1 Satz 2 VAG und Rn. 12ff. Rundschreiben Aufsichtsrechtliche Mindestanforderungen an die Geschäftsorganisation von Einrichtungen der betrieblichen Altersvorsorge [MaGo für EbAV]). Die Kriterien werden zusammenfassend als Profil bezeichnet.

~~10~~12 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.

II. Anforderungen

1. IT-Strategie

1.1. Die Geschäftsleitung hat eine mit der Geschäftsstrategie konsistente IT-Strategie festzulegen, in der die Ziele sowie die Maßnahmen zur Erreichung dieser Ziele dargestellt werden. ~~Die IT-Strategie ist durch die Geschäftsleitung~~Die Geschäftsleitung muss für die Umsetzung der IT-Strategie Sorge tragen. Die Geschäftsleitung hat zur Überwachung und Messung der Umsetzung der Ziele der Strategie sowie zu ihrer Beurteilung und Anpassung einen Prozess einzurichten. Dieser Prozess ist regelmäßig und anlassbezogen zu überprüfen und erforderlichenfalls anzupassen. ~~Die Geschäftsleitung muss für die Umsetzung der IT-Strategie Sorge tragen.~~

1.2. Der Detaillierungsgrad der IT-Strategie ist abhängig vom Risikoprofil des Unternehmens. Mindestinhalte ~~der IT-Strategie~~ sind:

(a) strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation des Unternehmens, der Ausgliederungen von IT-Dienstleistungen ~~oder der sonstigen Dienstleistungsbeziehungen im Bereich IT-Dienstleistungen~~und sonstige wichtige Abhängigkeiten von Dritten sowie zum isolierten Bezug von Hard- und/oder Software (zusammen auch „isolierter Bezug von IT“);

(b) Zuordnung der gängigen Standards, auf die das Unternehmen abstellt, auf die Bereiche der IT und der Informationssicherheit;

(c) Ziele, Zuständigkeiten und Einbindung der Informationssicherheit in die Organisation;

(d) strategische Entwicklung der IT-Architektur;

(e) Aussagen zum IT-Notfallmanagement unter Berücksichtigung der ~~IT-Belange~~Informationssicherheitsbelange;

~~IT-Dienstleister in diesem Sinne können auch die Trägerunternehmen von Einrichtungen der betrieblichen Altersversorgung sein.~~

Zu (a) Beschreibung der Rolle, der Positionierung und des Selbstverständnisses der IT im Hinblick auf Personaleinsatz und Budget der IT-Aufbau- und IT-Ablauforganisation sowie die Darstellung und strategische Einordnung der IT-Dienstleistungen~~;~~ und möglicher sonstiger wichtiger Abhängigkeiten von Dritten (wie z. B. Informations-, Telekommunikations- und Versorgungsdienstleistungen etc.);

Zu (b) Auswahl der gängigen Standards und Umsetzung auf die IT-Prozesse des Unternehmens sowie Darstellung des anvisierten Implementierungsumfangs der jeweiligen Standards;

Zu (c) Beschreibung der Bedeutung der Informationssicherheit im Unternehmen sowie der Einbettung der Informationssicherheit in die Fachbereiche und in das jeweilige Zusammenarbeitsmodell mit den IT-Dienstleistern. Dies beinhaltet auch grundlegende Aussagen zur Schulung und Sensibilisierung zur Informationssicherheit;

	(f) Aussagen zu den in den Fachbereichen selbst betriebenen und entwickelten ~~IT-Systemen~~Anwendungen.	Zu (d) Darstellung des Zielbilds der IT-Architektur. Ausgliederungen von IT-Dienstleistungen oder sonstigen Dienstleistungsbeziehungen im Bereich IT-Dienstleistungen sind angemessen in der IT-Strategie zu berücksichtigen. Den Unternehmen steht es frei, die Inhalte der IT-Strategie in einem gesonderten Dokument zusammenzufassen oder diese als Teilkapitel in die Geschäfts- oder Risikostrategie zu integrieren.
1.3.	Die in der IT-Strategie niedergelegten Ziele sind so zu formulieren, dass eine sinnvolle Überprüfung der Zielerreichung möglich ist.	
1.4.	Die IT-Strategie ist bei Erstverabschiedung sowie bei Anpassungen dem Aufsichtsorgan des Unternehmens zur Kenntnis zu geben und ggf. mit diesem zu erörtern.	~~Ob Erörterungsbedarf besteht, liegt im Ermessen des Aufsichtsorgans.~~
1.5.	Die Inhalte sowie Änderungen der IT-Strategie sind innerhalb des Unternehmens zeitnah und in geeigneter Weise zu kommunizieren.	

2. IT-Governance

2.1.	Die IT-Governance im Sinne dieses Rundschreibens ist die Struktur zur Steuerung sowie Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme einschließlich der dazugehörigen IT-Prozesse auf Basis der IT-Strategie. Hierfür maßgeblich sind insbesondere die Vorgaben zur IT-Aufbau- und IT-Ablauforganisation, zum Informationsrisiko- sowie Informationssicherheitsmanagement, zur quantitativ und qualitativ angemessenen ~~Personalausstattung~~Ressourcenausstattung der IT (personelle, finanzielle und sonstige Ressourcen) sowie zum Umfang und zur Qualität der technisch-organisatorischen Ausstattung. Die ~~Regelungen~~Leitlinien für die IT-Aufbau- und IT-Ablauforganisation sind bei wesentlichen Veränderungen der Aktivitäten und Prozesse zeitnah anzupassen.	

2.2.	Die Geschäftsleitung ist dafür verantwortlich, dass auf Basis der IT-Strategie die ~~Regelungen~~Leitlinien zur IT-Aufbau- und IT-Ablauforganisation festgelegt und bei Veränderungen der Aktivitäten und Prozesse zeitnah angepasst werden. Diese ~~Regelungen~~Leitlinien sind im Unternehmen entsprechend dem Risikoprofil zu treffen. Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen sowie Kommunikationswege sind klar zu definieren und aufeinander abzustimmen. Die Geschäftsleitung hat sicherzustellen, dass ~~die Regelungen zur IT-Aufbau- und IT-Ablauforganisation~~ diese Leitlinien wirksam umgesetzt werden. Dies gilt auch bezüglich der Schnittstellen zu wichtigen Ausgliederungen.	Die Geschäftsleitung hat den ~~Regelungen~~Leitlinien zur IT-Aufbau- und IT-Ablauforganisation zumindest bei Erstverabschiedung sowie bei ~~nicht geringfügigen~~wesentlichen Änderungen zuzustimmen. ~~Sollen geringfügige Änderungen vom Zustimmungserfordernis ausgenommen werden, hat das~~Das Unternehmen hat im Vorfeld festzulegen, welche Änderungen als ~~geringfügig~~wesentlich einzuschätzen sind. Die Vorgaben zur IT-Governance sind Bestandteil regelmäßiger Überprüfungen durch bezüglich IT hinreichend qualifizierte interne Revisoren.
2.3.	Die Informationsverarbeitung und -weitergabe in Geschäfts- und Serviceprozessen wird durch datenverarbeitende IT-Systeme und zugehörige IT-Prozesse unterstützt. Deren Umfang und Qualität hat sich am Risikoprofil zu orientieren.	
2.4.	Das Unternehmen hat insbesondere das Informationsrisikomanagement, das Informationssicherheitsmanagement, den IT-Betrieb und die Anwendungsentwicklung quantitativ und qualitativ angemessen mit ~~Personal~~Ressourcen auszustatten.	Hinsichtlich der Maßnahmen zur Erhaltung einer angemessenen qualitativen ~~Personalausstattung~~Ressourcenausstattung (personelle, finanzielle und sonstige Ressourcen) werden insbesondere der Stand der Technik sowie die aktuelle und zukünftige ~~Entwicklung der~~ Bedrohungslage berücksichtigt.
2.5.	Alle Mitarbeiter müssen fortlaufend - abhängig von ihren Aufgaben, Kompetenzen und Verantwortlichkeiten - über die erforderlichen Kenntnisse und Erfahrungen, auch im Bereich der IT, verfügen.	Durch geeignete Maßnahmen ist zu gewährleisten, dass das Qualifikationsniveau der Mitarbeiter angemessen ist.

2.6.	Die Abwesenheit oder das Ausscheiden von Mitarbeitern darf nicht zu nachhaltigen Störungen der Betriebsabläufe führen.	
2.7.	Interessenkonflikte innerhalb der IT-Aufbau- und IT-Ablauforganisation sind zu vermeiden.	Bei der Ausgestaltung der IT-Aufbau- und IT-Ablauforganisation ist sicherzustellen, dass miteinander unvereinbare Tätigkeiten durch unterschiedliche Mitarbeiter durchgeführt werden. Interessenkonflikten zwischen Aktivitäten, die beispielsweise im Zusammenhang mit der Anwendungsentwicklung und den Aufgaben des IT-Betriebs stehen, kann durch aufbau- oder ablauforganisatorische Maßnahmen, beispielsweise durch eine adäquate Rollendefinition, begegnet werden.
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~~, und deren~~. Die Einhaltung der Kriterien ist zu überwachen.	Bei der Festlegung der Kriterien können z. B. die Qualität der ~~Leistungserbringungen~~Leistungserbringung, die Verfügbarkeit, Wartbarkeit, Anpassbarkeit an neue Anforderungen, Sicherheit der IT-Systeme oder der dazugehörigen IT-Prozesse sowie deren Kosten berücksichtigt werden.
2.9.	Umfang und Qualität der technisch-organisatorischen Ausstattung haben sich am Risikoprofil zu orientieren.	
2.10.	Die IT-Systeme und die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen~~,~~; insbesondere sind Prozesse für eine angemessene Berechtigungsvergabe einzurichten, die sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätig-	

	keit benötigt~~; die~~. Die Zusammenfassung von Berechtigungen in einem Rollenmodell ist möglich. Die Eignung der IT-Systeme und der zugehörigen IT-Prozesse, die Schutzziele zu erreichen, ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.	
2.11.	Das Unternehmen hat sicherzustellen, dass die IT-bezogenen Geschäftsaktivitäten auf der Grundlage von Arbeitsablaufbeschreibungen (Organisationsrichtlinien) betrieben werden. Der Detaillierungsgrad der Organisationsrichtlinien hängt vom Risikoprofil ab.	Hinsichtlich der Darstellung der Organisationsrichtlinien kommt es in erster Linie darauf an, dass diese sachgerecht und für die Mitarbeiter des Unternehmens nachvollziehbar sind. Die konkrete Art der Darstellung bleibt dem Unternehmen überlassen. Die Organisationsrichtlinien werden in ihrer aktuellen Form durch den zuständigen Kompetenzträger in Kraft gesetzt.

3. Informationsrisikomanagement

3.1.	Das Unternehmen hat im Rahmen des Risikomanagements die mit dem Management der Informationsrisiken verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege zu definieren und aufeinander abzustimmen. Das Unternehmen hat angemessene Identifikations-, Bewertungs-, Überwachungs- und Steuerungsprozesse einzurichten und diesbezügliche Berichtspflichten zu definieren.	
3.2.	Die Identifikations-, Bewertungs-, Überwachungs- und Steuerungsprozesse haben 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 von Maßnahmen zur Risikobehandlung der verbliebenen Restrisiken zu umfassen.	Die Risikokriterien berücksichtigen die Kritikalität der Geschäftsprozesse und -aktivitäten sowie bekannte Gefährdungen und Vorfälle, welche das Unternehmen bereits in der Vergangenheit beeinflusst haben.

3.3.	Das Risikomanagement der Informationsrisiken ist unter Mitwirkung aller maßgeblichen Stellen und Funktionen kompetenzgerecht und frei von Interessenkonflikten umzusetzen.	Zu den maßgeblichen Stellen gehören auch die Fachbereiche, die Eigentümer der Informationen oder der Informationsrisiken sind.
3.4.	Das Unternehmen hat über einen aktuellen Überblick über die Bestandteile des festgelegten Informationsverbunds sowie deren Abhängigkeiten und Schnittstellen zu verfügen.	Zu einem Informationsverbund gehören beispielsweise geschäftsrelevante Informationen, ~~Geschäftsprozesse~~Geschäfts- und Unterstützungsprozesse, IT-Systeme und die zugehörigen IT-Prozesse sowie Netz- und Gebäudeinfrastrukturen. Abhängigkeiten und Schnittstellen berücksichtigen auch die Vernetzung des Informationsverbundes mit Dritten.
3.5.	~~Die Methodik zur Ermittlung des Schutzbedarfs (~~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~~") hat die Konsistenz der resultierenden Schutzbedarfe nachvollziehbar sicherzustellen.~~", zu ermitteln. Die Eigentümer der Informationen bzw. die Fachbereiche, die verantwortlich für die Geschäftsprozesse sind, verantworten die Ermittlung des Schutzbedarfs.	~~Schutzbedarfskategorien sind beispielhaft „Niedrig“, „Mittel“, „Hoch“ und „Sehr hoch“.~~
3.6.	Die Schutzbedarfsfeststellung sowie die zugehörige Dokumentation sind durch das Informationsrisikomanagement angemessen zu überprüfen.	

3.6.3.7. ~~Die~~Das Unternehmen hat Anforderungen ~~des Unternehmens~~zu definieren, die zur ~~Umsetzung der Schutzziele in den Schutzbedarfskategorien~~Erreichung des jeweiligen Schutzbedarfs angemessen sind ~~durch das Unternehmen festzulegen und~~und diese in geeigneter Form zu dokumentieren (Sollmaßnahmenkatalog).	Der Sollmaßnahmenkatalog enthält lediglich die Anforderung, nicht jedoch deren konkrete Umsetzung.
3.7.3.8. ~~Auf~~Das Unternehmen hat auf Basis der festgelegten ~~IT-~~Risikokriterien ~~hat~~regelmäßig eine Risikoanalyse durchzuführen. Die Risikoanalyse ist zu ~~erfolgen~~koordinieren und zu dokumentieren. Risikoreduzierende Maßnahmen aufgrund unvollständig umgesetzter Sollmaßnahmen sind wirksam zu koordinieren, zu dokumentieren, zu überwachen und zu steuern. Die Ergebnisse der Risikoanalyse sind ~~zu genehmigen und~~ in den Prozess des Managements der operationellen Risiken zu überführen. Die Behandlung der Risiken ist kompetenzgerecht zu genehmigen.	~~IT-~~Risikokriterien enthalten beispielsweise mögliche Bedrohungen, das Schadenspotenzial, die Schadenshäufigkeit sowie den Risikoappetit. Die Risikoanalyse ~~kann u. a. auch~~erfolgt auf Grundlage eines Vergleichs der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen ~~erfolgen.~~(Soll-Ist-Vergleich).
3.9. Das Unternehmen informiert sich laufend über Bedrohungen und Schwachstellen seines Informationsverbundes, prüft ihre Relevanz, bewertet ihre Auswirkung und ergreift, sofern erforderlich, geeignete technische und organisatorische Maßnahmen.	Hierbei sind interne und externe Veränderungen (z. B. der Bedrohungslage) zu berücksichtigen.
3.8.3.10. Die Geschäftsleitung ist regelmäßig, mindestens jedoch jährlich~~,~~ und ggf. ad hoc, insbesondere über die Ergebnisse der Risikoanalyse in einem schriftlichen Bericht zu unterrichten. Unterjährig ist die Geschäftsleitung, ggf. der zuständige Geschäftsleiter, mindestens vierteljährlich per Statusbericht zu informieren.	Der Statusbericht enthält beispielsweise die Bewertung der Risikosituation im Vergleich zum Vorbericht. Die Risikosituation enthält auch externe potenzielle Bedrohungen.

4. Informationssicherheitsmanagement

4.1. Das Informationssicherheitsmanagement macht Vorgaben zur Informationssicherheit, definiert entsprechende Prozesse und steuert deren Umsetzung. Das Informationssicherheitsmanagement folgt einem fortlaufenden Prozess, der die Phasen Planung, Umsetzung, Erfolgskontrolle sowie Optimierung umfasst.

4.2. Die Geschäftsleitung hat eine schriftliche Informationssicherheitsleitlinie zu beschließen und innerhalb des Unternehmens ~~angemessen~~ zu kommunizieren. Die Informationssicherheitsleitlinie hat im Einklang mit den Strategien des Unternehmens zu stehen. Die Leitlinie ist bei wesentlichen Veränderungen der Rahmenbedingungen zu prüfen und bei Bedarf zeitnah anzupassen.

In der Informationssicherheitsleitlinie werden die ~~Ziele~~Eckpunkte zum Schutz von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität sowie der Geltungsbereich für die Informationssicherheit festgelegt ~~und~~. Darüber hinaus werden die wesentlichen organisatorischen Aspekte, wie die wichtigsten Rollen und Verantwortlichkeiten des Informationssicherheitsmanagements, beschrieben. ~~Regelmäßige Überprüfungen~~Mit der Leitlinie legt die Geschäftsleitung u. a. dar:

- ihre Gesamtverantwortung für die Informationssicherheit,
- Frequenz und ~~Anpassungen~~Umfang des Berichtswesens zur Informationssicherheit,
- die Kompetenzen im Umgang mit Informationsrisiken,
- die grundlegenden Anforderungen der Informationssicherheit an ~~geänderte Bedingungen werden risikoorientiert vorgenommen.~~Personal, Auftragnehmer, Prozesse und Technologien,
- geeignete Kriterien für die Information der Geschäftsleitung über Informationssicherheitsvorfälle, sofern diese Kriterien nicht in einer Informationssicherheitsrichtlinie dargelegt werden.

Rahmenbedingungen umfassen u. a. interne Veränderungen der IT-Aufbau- und IT-Ablauforganisation ~~sowie~~oder der IT-Systeme ~~einer Institution (Geschäftsprozesse, Fachaufgaben, organisatorische Gliederung) werden hierbei~~

		~~ebenso berücksichtigt wie~~ des Versicherungsunternehmens sowie äußere Veränderungen ~~der äußeren Rahmenbedingungen~~ (z. B. ~~gesetzliche Regelungen, regulatorische Anforderungen), der~~ Bedrohungsszenarien, Technologien oder ~~der Sicherheitstechnologien.~~rechtliche Anforderungen).
4.3.	Auf Basis der Informationssicherheitsleitlinie und der Ergebnisse des Informationsrisikomanagements sind konkretisierende, den Stand der Technik berücksichtigende Informationssicherheitsrichtlinien und Informationssicherheitsprozesse ~~mit den Teilprozessen Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung zu definieren.~~zu definieren.	Informationssicherheitsrichtlinien werden ~~beispielsweise~~z. B. für die Bereiche Netzwerksicherheit, Kryptografie, ~~Authentisierung~~Identitäts- und Rechtemanagement, Protokollierung sowie physische Sicherheit (z. B. Perimeter- und Gebäudeschutz) erstellt. Informationssicherheitsprozesse dienen in erster Linie der Erreichung der vereinbarten Schutzziele. Dazu gehört u. a., Informationssicherheitsvorfällen vorzubeugen ~~und~~bzw. diese zu identifizieren sowie die angemessene Reaktion und Kommunikation im weiteren Verlauf. Zu den Ergebnissen des Informationsrisikomanagements zählen u. a die definierten Sollmaßnahmen (vgl. 3.7).
4.4.	Das Unternehmen 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), ■ die Art, Umfang und Frequenz von Tests und Überprüfungen, ■ Zuständigkeiten und Regelungen zur Vermeidung von Interessenkonflikten.

4.4.4.5. ~~Das Unternehmen~~Die Geschäftsleitung hat die Funktion des Informationssicherheitsbeauftragten einzurichten. Diese überwachende Funktion umfasst die Wahrnehmung aller Belange der Informationssicherheit innerhalb des Unternehmens und gegenüber Dritten. Sie stellt sicher, dass die in der IT-Strategie, der Informationssicherheitsleitlinie und den Informationssicherheitsrichtlinien des Unternehmens ~~niedergelegten~~festgelegten Ziele und Maßnahmen hinsichtlich der Informationssicherheit sowohl intern als auch - sofern und soweit geboten - gegenüber Dritten transparent gemacht und deren Einhaltung regelmäßig sowie anlassbezogen überprüft und überwacht werden.

Diese überwachende Funktion kann durch eine oder mehrere natürliche Personen abgebildet werden, wobei einer dieser Personen die Verantwortung dafür zukommt, dass die Funktion ihre Aufgaben ordnungsgemäß erfüllt. Es ist nicht zulässig, diese Verantwortung auf mehrere natürliche Personen aufzuspalten.

Die Funktion des Informationssicherheitsbeauftragten umfasst insbesondere die nachfolgenden Aufgaben:

- die Geschäftsleitung beim Festlegen und Anpassen der Informationssicherheitsleitlinie zu unterstützen und in allen Fragen der Informationssicherheit zu beraten; dies umfasst auch Hilfestellungen bei der Lösung von Zielkonflikten (z. B. Wirtschaftlichkeit kontra Informationssicherheit),
- Erstellung von Informationssicherheitsrichtlinien und ggf. weiteren einschlägigen Regelungen sowie die Kontrolle ihrer Einhaltung,
- den Informationssicherheitsprozess im Unternehmen zu steuern und zu koordinieren sowie diesen gegenüber IT-Dienstleistern zu überwachen und bei allen damit zusammenhängenden Aufgaben mitzuwirken,
- die Beteiligung bei der Erstellung und Fortschreibung des Notfallkonzepts bzgl. ~~der IT-Belange~~der Informationssicherheitsbelange,
- die Realisierung von Informationssicherheitsmaßnahmen zu initiieren und zu überwachen,
- ~~angemessene Beteiligung bei Projekten mit IT-Relevanz (je nach Einzelfall kann eine angemessene Beteiligung reichen von der Information des Informationssicherheitsbeauftragten über das IT-Projekt bis hin zu seiner aktiven Mitwirkung daran),~~

	■ Überwachung und Hinwirkung auf Einhaltung der Informationssicherheit bei Projekten und Beschaffungen, ■ als Ansprechpartner für Fragen der Informationssicherheit innerhalb des Unternehmens und für Dritte bereitzustehen, ■ Informationssicherheitsvorfälle zu untersuchen und ~~diesbezüglich~~ an die Geschäftsleitung zu berichten ~~(zuvor hat das Unternehmen geeignete Kriterien für die Information der Geschäftsleitung über Informationssicherheitsvorfälle festzulegen),~~. ■ Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und zu koordinieren. Der Informationssicherheitsbeauftragte kann durch ein Informationssicherheitsmanagement-Team unterstützt werden.
~~4.5.~~4.6. Die Funktion des Informationssicherheitsbeauftragten ist aufbau- und ablauforganisatorisch angemessen unabhängig auszugestalten, um mögliche Interessenskonflikte zu vermeiden.	Unternehmen können, wenn dies dem Risikoprofil entspricht, die Funktion des Informationssicherheitsbeauftragten mit anderen Funktionen im Unternehmen kombinieren. Zur Vermeidung möglicher Interessenkonflikte werden zudem insbesondere folgende Maßnahmen beachtet: ■ Funktions- und Stellenbeschreibung für den Informationssicherheitsbeauftragten, seinen Vertreter und ggf. weitere Stellen, ■ Festlegung der erforderlichen Ressourcenausstattung für die Funktion des Informationssicherheitsbeauftragten, ■ ein der Funktion zugewiesenes Budget für ~~Informationssicherheitsschulungen~~Informationssicherheitsschulungen im Unternehmen und die persönliche Weiterbildung des Informationssicherheitsbeauftragten

	sowie seines Vertreters und ggf. des Informationssicherheitsmanagement-Teams, ■ unmittelbare und jederzeitige Gelegenheit zur Berichterstattung des Informationssicherheitsbeauftragten an die Geschäftsleitung, ■ Verpflichtung der Beschäftigten des Unternehmens sowie der IT-Dienstleister zur sofortigen und umfassenden Unterrichtung des Informationssicherheitsbeauftragten über alle bekannt gewordenen ~~IT-sicherheitsrelevanten~~informationssicherheitsrelevanten Sachverhalte, die das Unternehmen betreffen~~.~~, ■ ~~Die~~die Funktion des Informationssicherheitsbeauftragten wird ~~aufbau- und ablauforganisatorisch~~ angemessen von den Bereichen getrennt, die für den Betrieb und die Weiterentwicklung der IT-Systeme zuständig sind~~.~~, ■ ~~Der~~der Informationssicherheitsbeauftragte nimmt keine Aufgaben der internen Revision wahr.
~~4.6.~~4.7. Jedes Unternehmen sollte die Funktion des Informationssicherheitsbeauftragten im eigenen Unternehmen vorhalten.	Bei Ausgliederung der Funktion des Informationssicherheitsbeauftragten sind die hierfür jeweils geltenden Anforderungen zu erfüllen. Bei der Entscheidung für oder gegen die Ausgliederung hat das Unternehmen das Ausmaß zu berücksichtigen, in dem IT-bezogene Geschäftsaktivitäten im eigenen Unternehmen oder durch externe Dienstleister betrieben werden. Aufbauend auf dieser Betrachtung muss die Frage eine Rolle spielen, wie eine sachgerechte Funktionsausübung des Informationssicherheitsbeauftragten gewährleistet werden kann.

4.7.4.8.	Nach einem Informationssicherheitsvorfall sind die Auswirkungen auf die Informationssicherheit zeitnah zu analysieren und angemessene Nachsorgemaßnahmen zu veranlassen.	Die Definition des Begriffes „Informationssicherheitsvorfall“ nach Art und Umfang ~~basiert auf dem~~orientiert sich am Schutzbedarf der betroffenen ~~Geschäftsprozesse, IT-Systeme und den zugehörigen IT-Prozessen~~Bestandteile des Informationsverbundes. Ein Informationssicherheitsvorfall kann auch dann vorliegen, wenn mindestens eines der Schutzziele („Verfügbarkeit“, „Integrität“, „Vertraulichkeit“, „Authentizität") gemäß den Vorgaben des unternehmensspezifischen Sollkonzepts der Informationssicherheit ~~– über dem definierten Schwellenwert –~~ verletzt ist. ~~Der Begriff~~Die Begriffe „Informationssicherheitsvorfall~~“ ist nachvollziehbar vom Begriff „~~“, „sicherheitsrelevantes Ereignis“ (im Sinne der operativen Informationssicherheit) und „ungeplante Abweichung vom Regelbetrieb“ (im Sinne von „Störung ~~im Tagesbetrieb“) abzugrenzen~~“) werden nachvollziehbar voneinander abgegrenzt.
4.9.	Das Unternehmen hat ein kontinuierliches und angemessenes Sensibilisierungs- und Schulungsprogramm für Informationssicherheit festzulegen. Das Programm ist regelmäßig auf Aktualität und Angemessenheit hin zu überprüfen.	Das Programm sollte zielgruppenorientiert 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).
~~4.8.~~4.10.	Der Informationssicherheitsbeauftragte hat der Geschäftsleitung, ggf. dem zuständigen Geschäftsleiter, regelmäßig, mindestens	Der Statusbericht enthält beispielsweise die Bewertung der Informationssicherheitslage im Vergleich zum Vorbericht, Informationen zu Projekten zur

	vierteljährlich~~,~~ und ggf. ad hoc, über den Status der Informationssicherheit zu berichten.	Informationssicherheit, Informationssicherheitsvorfälle sowie ~~Penetrationstest-Ergebnisse.~~Penetrationstestergebnisse.

5. ~~Benutzerberechtigungsmanagement~~Operative Informationssicherheit

5.1. Die operative Informationssicherheit setzt die Anforderungen des Informationssicherheitsmanagements um. 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.

5.2. Das Unternehmen hat 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, Verfügbarkeitsangriffen oder vor nicht autorisiertem Zugriff),
- Perimeterschutz von z. B. Liegenschaften, Rechenzentren und anderen sensiblen Bereichen.

5.3.	Gefährdungen des Informationsverbundes sind 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.
5.4.	Im Rahmen der Überwachung der Informationssicherheit ist ein angemessenes Portfolio an Regeln zur Identifizierung sicherheitsrelevanter Ereignisse zu definieren. Regeln sind vor Inbetriebnahme zu testen. Die Regeln sind 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
5.5.	Sicherheitsrelevante Ereignisse sind zeitnah zu analysieren und auf daraus resultierende Informationssicherheitsvorfälle ist unter Verantwortung des Informationssicherheitsmanagements angemessen zu reagieren.	Sicherheitsrelevante Ereignisse ergeben sich beispielsweise aus der regelbasierten Auswertung der potentiell sicherheitsrelevanten Informationen.
5.6.	Die Sicherheit der IT-Systeme ist regelmäßig, anlassbezogen und unter Vermeidung von Interessenskonflikten zu überprüfen. 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-Analyse),

- Schwachstellenscans,
- Penetrationstests,
- Simulationen von Angriffen.

6. Identitäts- und Rechtemanagement

5.1.6.1. Das Unternehmen hat ein ~~Benutzerberechtigungsmanagement~~Identitäts- und Rechtemanagement einzurichten, welches sicherstellt, dass den Benutzern eingeräumte Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben des Unternehmens entspricht. Bei der Ausgestaltung des ~~Benutzerberechtigungsmanagements~~Identitäts- und Rechtemanagements sind die Anforderungen an die Ausgestaltung der Prozesse (siehe ~~II. Rn. 7 und 15)~~2.2 und 2.10) entsprechend zu berücksichtigen. Jegliche Zugriffs-, Zugangs- und Zutrittsrechte auf Bestandteile bzw. zu Bestandteilen des Informationsverbundes müssen standardisierten Prozessen und Kontrollen unterliegen.

5.2.6.2. ~~Im Rahmen des Benutzerberechtigungsmanagements legen~~ Berechtigungskonzepte legen den Umfang und die Nutzungsbedingungen der Berechtigungen für die IT-Systeme (Zugang zu IT-Systemen sowie Zugriff auf Daten) sowie die Zutrittsrechte zu Räumen konsistent zum ermittelten Schutzbedarf sowie vollständig und nachvollziehbar ableitbar für alle ~~von einem IT-System~~ bereitgestellten Berechtigungen fest. Berechtigungskonzepte haben ~~im Hinblick auf~~ die Vergabe von Berechtigungen ~~an Benutzer~~nach dem Sparsamkeitsgrundsatz („Need-to-know“ und „Least-Privilege“ Prinzipien) sicherzustellen~~, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt~~; die Zusammenfassung von Berechtigungen in einem Rollenmodell ist möglich. Berechtigungskonzepte haben des Weiteren die Funktionstrennung auch berechtigungskonzeptübergreifend zu wahren und Interessenskonflikte ~~des Personals~~ zu vermeiden. Bei Eine mögliche Nutzungsbedingung ist die Befristung der eingeräumten Berechtigungen. Berechtigungen können ~~sowohl~~, je nach Art, für personalisierte~~,~~ sowie für nicht personalisierte ~~als auch für~~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.

Zugriffsrechte:

Die eingerichteten Berechtigungen dürfen nicht im Widerspruch zur organisatorischen Zuordnung von Mitarbeitern stehen. Insbesondere bei Berechtigungsvergaben im Rahmen von Rollenmodellen ist darauf zu achten, dass Funktionstrennungen beibehalten bzw. Interessenkonflikte vermieden werden.

IT-gestützter Bearbeitung ist die Funktionstrennung durch entsprechende Verfahren und Schutzmaßnahmen sicherzustellen. Berechtigungskonzepte sind regelmäßig und anlassbezogen zu überprüfen und ggf. zu aktualisieren.	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 sind zu löschen.
5.3.6.3. ~~Nicht personalisierte Berechtigungen~~Zugriffe und Zugänge müssen jederzeit zweifelsfrei einer handelnden ~~natürlichen~~bzw. verantwortlichen Person (möglichst automatisiert) zuzuordnen sein. ~~Abweichungen in begründeten Ausnahmefällen und die hieraus resultierenden Risiken sind zu genehmigen und zu dokumentieren.~~	Beispielsweise müssen automatisierte Aktivitäten 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.
~~Jeder technische Benutzer muss einer verantwortlichen natürlichen Person zugeordnet sein.~~	
5.4.6.4. Die Verfahren zur Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen für Benutzer haben durch Genehmigungs- und Kontrollprozesse sicherzustellen, dass die Vorgaben des Berechtigungskonzepts eingehalten werden. Dabei ist die fachlich verantwortliche Stelle so einzubinden, dass sie ihrer fachlichen Verantwortung nachkommen kann.	Die Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen umfassen jeweils ~~die~~auch die zeitnahe oder unverzügliche Umsetzung ~~des Berechtigungsantrags~~ im Zielsystem. Grund für eine unverzügliche Deaktivierung bzw. Löschung von Berechtigungen ist u. a. die Gefahr einer missbräuchlichen Verwendung (z. B. bei fristloser Kündigung eines Mitarbeiters). Bei Einrichtung und Änderung von Berechtigungen bedarf es der vorherigen Zustimmung der fachlich verantwortlichen Stelle, bei Deaktivierung oder Löschung ist sie zeitnah zu informieren.

~~5.5.~~6.5. Berechtigungen sind bei Bedarf zeitnah anzupassen. Dies beinhaltet auch die regelmäßige und anlassbezogene Überprüfung innerhalb angemessener Fristen, ob die eingeräumten Berechtigungen weiterhin benötigt werden und ob diese den Vorgaben des Berechtigungskonzepts entsprechen (Rezertifizierung). Bei der Rezertifizierung sind die für die Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen zuständigen Kontrollinstanzen ~~mit einzubeziehen.~~miteinzubeziehen.	Wesentliche Berechtigungen sind mindestens jährlich zu überprüfen, alle anderen mindestens alle drei Jahre. Besonders kritische Berechtigungen, wie sie beispielsweise Administratoren aufweisen, sind mindestens halbjährlich zu überprüfen. Fällt im Rahmen der Rezertifizierung auf, dass ~~außerhalb des vorgeschriebenen Verfahrens~~nicht legitimierte Berechtigungen ~~eingeräumt wurden~~vorhanden sind, so werden diese gemäß ~~der~~ Regelverfahren ~~zur Einrichtung, Änderung und Löschung von Berechtigungen~~zeitnah entzogen und bei Bedarf weitere Maßnahmen (z. B. Ursachenanalyse, Vorfallsmeldung) ergriffen.
~~5.6.~~6.6. Die Einrichtung, Änderung, Deaktivierung sowie Löschung von Berechtigungen und die Rezertifizierung sind nachvollziehbar und auswertbar zu dokumentieren.	
~~5.7.~~6.7. Das Unternehmen hat nach Maßgabe des Schutzbedarfs und der ~~Soll-Anforderungen~~Sollanforderungen Prozesse zur Protokollierung und Überwachung einzurichten, die überprüfbar machen, dass die Berechtigungen nur wie vorgesehen eingesetzt werden. Aufgrund der damit verbundenen weitreichenden Eingriffsmöglichkeiten hat das Unternehmen insbesondere für die Aktivitäten mit privilegierten (besonders kritischen) Benutzer- und Zutrittsrechten angemessene Prozesse zur Protokollierung und Überwachung einzurichten.	Die übergeordnete Verantwortung für die Prozesse zur Protokollierung und Überwachung von Berechtigungen wird einer Stelle zugeordnet, die unabhängig vom berechtigten Benutzer oder dessen Organisationseinheit ist. ~~Aufgrund weitreichender Eingriffsmöglichkeiten privilegierter Benutzer wird das Unternehmen insbesondere für deren Aktivitäten angemessene Prozesse zur Protokollierung und Überwachung einrichten.~~ Zu privilegierten Zutrittsrechten zählen in der Regel die Rechte zum Zutritt zu Rechenzentren, Technikräumen sowie sonstigen sensiblen Bereichen.
~~5.8.~~6.8. Durch begleitende technisch-organisatorische Maßnahmen ist einer Umgehung der Vorgaben der Berechtigungskonzepte vorzubeugen.	Technisch-organisatorische Maßnahmen hierzu sind beispielsweise: ■ Auswahl angemessener Authentifizierungsverfahren~~,~~ (u. a. starke Authentifizierung im Falle von Fernzugriffen),

- Implementierung einer Richtlinie zur Wahl sicherer Passwörter,
- ~~automatischer passwortgesicherter Bildschirmschoner,~~
- automatische passwortgesicherte Bildschirmsperre,
- Verschlüsselung von Daten,
- ~~eine~~ manipulationssichere Implementierung der Protokollierung,
- Maßnahmen zur Sensibilisierung der Mitarbeiter.

~~6.~~7. IT-Projekte~~,~~ und Anwendungsentwicklung ~~(inkl. durch Endbenutzer in den Fachbereichen)~~

~~6.1.~~7.1. Wesentliche Veränderungen in den IT-Systemen im Rahmen von IT-Projekten, deren Auswirkung auf die IT-Aufbau- und IT-Ablauforganisation sowie die dazugehörigen IT-Prozesse sind vorab im Rahmen einer ~~Auswirkungsanalyse~~Analyse zu bewerten. Dabei hat das Unternehmen insbesondere die Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität zu analysieren. In diese Analysen sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten zu beteiligen. Im Rahmen ihrer Aufgaben sind auch die unabhängige Risikocontrollingfunktion, die Compliance-Funktion und die versicherungsmathematische Funktion zu beteiligen, sofern das Unternehmen die jeweiligen Funktionen von Gesetzes wegen einzurichten hat. Die Funktion der internen Revision kann beratend beteiligt werden. Die Sätze 1 bis 5 gelten auch im Hinblick auf den erstmaligen Einsatz sowie wesentliche Veränderungen von IT-Systemen.

~~6.2.~~7.2. Die IT-Systeme sind vor ihrer Übernahme in den produktiven Betrieb zu testen und von den fachlich sowie auch von den technisch zuständigen Mitarbeitern abzunehmen. Hierfür ist ein Regelprozess der Entwicklung, des Testens, der Freigabe und der Implementierung in die Produktionsprozesse zu etablieren. ~~Produktions- und Testumgebung~~ Produktionsumgebungen sind ~~dabei~~ grundsätzlich ~~voneinander~~von Entwicklungs- und Testumgebungen zu trennen. Diese Anforderungen gelten grundsätzlich auch bei wesentlichen Veränderungen der IT-Systeme.

Soweit Änderungen an IT-Systemen automatisiert von Dritten durchgeführt werden und nicht vor Inbetriebnahme im Unternehmen getestet werden können, überzeugt sich das Unternehmen regelmäßig davon, dass bei diesem Dritten die notwendigen Tests vorab durchgeführt werden.

6.3.7.3. ~~Die Anforderungen unter II. Rn. 14, 15, 18 und 43~~Die Anforderungen unter Kap. 2.9, 2.10, 3.2 und 7.2 sind auch beim Einsatz von durch die Fachbereiche selbst entwickelten Anwendungen (Individuelle Datenverarbeitung - „IDV“) entsprechend der Kritikalität der unterstützten Geschäftsprozesse und der Bedeutung der Anwendungen für diese Prozesse zu beachten. Die Festlegung von Maßnahmen zur Sicherstellung der Datensicherheit hat sich am Schutzbedarf der verarbeiteten Daten zu orientieren.	Dies gilt auch für den erstmaligen Einsatz sowie für wesentliche Veränderungen von ~~IT-Systemen~~Anwendungen.
6.4.7.4. Die organisatorischen Grundlagen ~~von~~für IT-~~Projekten (inkl. Qualitätssicherungsmaßnahmen)~~Projekte und die Kriterien für deren Anwendung sind angemessen zu regeln.	IT-Projekte sind Projekte, die mit Anpassungen der IT-Systeme einhergehen. Der Ausgangspunkt kann sowohl im Fachbereich als auch im IT-Bereich liegen. Organisatorische Grundlagen berücksichtigen 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).

6.5.7.5. IT-Projekte sind ~~angemessen zu steuern, insbesondere~~ unter Berücksichtigung ~~der~~ ihrer Ziele und Risiken im Hinblick auf die Dauer, ~~den Ressourcenverbrauch~~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.	Beispielsweise kann die Entscheidung über den Übergang zwischen den Projektphasen bzw. Projektabschnitten von eindeutigen Qualitätskriterien des jeweiligen Vorgehensmodells abhängen.
6.6.7.6. Das Portfolio der IT-Projekte ist angemessen zu überwachen und zu steuern. Dabei ist zu berücksichtigen, dass auch aus Abhängigkeiten verschiedener Projekte voneinander Risiken resultieren können.	Die Portfoliosicht ermöglicht einen Überblick über die IT-Projekte mit den entsprechenden Projektdaten, Ressourcen, Risiken und Abhängigkeiten.
6.7.7.7. ~~Wesentliche~~Über wesentliche IT-Projekte und IT-Projektrisiken ~~sind~~ wird der Geschäftsleitung regelmäßig und anlassbezogen ~~zu berichten~~berichtet. IT-Projektrisiken sind im Risikomanagement angemessen zu berücksichtigen.	
6.8.7.8. Für die Anwendungsentwicklung sind angemessene Prozesse festzulegen, die Vorgaben zur Anforderungsermittlung, zum Entwicklungsziel, zur (technischen) Umsetzung (einschließlich Programmierrichtlinien), zur Qualitätssicherung sowie zu Test, Abnahme und Freigabe enthalten.	Anwendungsentwicklung umfasst ~~beispielsweise~~u.a. die ~~extern oder im Unternehmen entwickelten Anwendungen (z. B.~~Erstellung von Software für Geschäfts- und Unterstützungsprozesse (einschließlich individueller Datenverarbeitung – IDV). Die Ausgestaltung der Prozesse erfolgt entsprechend dem Risikoprofil.

~~6.9.~~7.9. Sowohl Anforderungen an die Funktionalität der Anwendung wie auch nichtfunktionale Anforderungen müssen ~~sachgerecht~~ erhoben, bewertet und dokumentiert werden. Zu jeder Anforderung sind entsprechende Akzeptanz- und Testkriterien zu definieren. Die Verantwortung für die Erhebung und Bewertung der Anforderungen ~~liegt in den Fachbereichen~~(funktional und nichtfunktional) haben die fachlich verantwortlichen Stellen zu tragen.	Anforderungsdokumente ~~entsprechend dem gewählten Vorgehen sind~~können sich nach Vorgehensmodell unterscheiden und beinhalten beispielsweise: ■ Fachkonzept (~~beispielsweise User-Story~~Lastenheft), ■ ~~Technisches~~technisches Fachkonzept (~~beispielsweise~~ Pflichtenheft ~~oder~~), ■ User Story/Product Back-Log~~).~~. Nichtfunktionale Anforderungen an IT-Systeme sind beispielsweise: ~~■ Ergebnisse der Schutzbedarfsfeststellung,~~ ■ Anforderungen an die Informationssicherheit, ■ Zugriffsregelungen, ■ Ergonomie, ■ Wartbarkeit, ■ Antwortzeiten, ■ Resilienz.
~~6.10.~~7.10. Im Rahmen der Anwendungsentwicklung sind je nach ~~Maßgabe des Schutzbedarfs~~Schutzbedarf angemessene Vorkehrungen ~~im Hinblick darauf~~ zu treffen, dass ~~nach Produktivsetzung der~~auch im produktiven Betrieb einer Anwendung die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten nachvollziehbar sichergestellt werden.	Geeignete Vorkehrungen können sein: ■ Prüfung der Eingabedaten, ■ Systemzugangskontrolle, ■ ~~Nutzer-Authentifizierung~~Benutzerauthentifizierung, ■ Transaktionsautorisierung,

	■ Protokollierung der Systemaktivität, ■ Prüfpfade (Audit Logs), ■ Verfolgung von sicherheitsrelevanten Ereignissen, ■ Behandlung von Ausnahmen.
~~6.11.~~7.11. ~~Im Rahmen der Anwendungsentwicklung müssen~~Die Integrität der Anwendung (insbesondere des Quellcodes) ist angemessen sicherzustellen. Zudem müssen u. a. Vorkehrungen getroffen werden, die erkennen lassen, ob eine Anwendung versehentlich geändert oder absichtlich manipuliert wurde.	Eine geeignete Vorkehrung unter Berücksichtigung des Schutzbedarfs kann die Überprüfung des Quellcodes ~~im Rahmen der Anwendungsentwicklung sein.~~sein. Die Überprüfung des Quellcodes ist eine methodische Untersuchung zur Identifizierung von Risiken.
~~6.12.~~7.12. Sowohl die von Dritten für das Unternehmen ~~entwickelte~~entwickelten als auch die im Unternehmen selbst ~~entwickelte Anwendung ist~~entwickelten Anwendungen sind übersichtlich und für sachkundige Dritte nachvollziehbar zu dokumentieren.	Die Dokumentation ~~der~~einer Anwendung ~~und ihrer Entwicklung muss zumindest~~umfasst mindestens folgende ~~Fragen klären~~Inhalte: ~~■ Was soll entwickelt werden?~~ ~~■ Wie wurde die Anwendung sowohl technisch als auch prozessual entwickelt?~~ ~~■ Wie muss die Anwendung betrieben und eingesetzt werden?~~ ■ Anwenderdokumentation, ■ technische Systemdokumentation, ■ Betriebsdokumentation. Zur Nachvollziehbarkeit der Anwendungsentwicklung trägt beispielsweise eine Versionierung des Quellcodes und der Anforderungsdokumente bei.

6.13.7.13. Es ist eine Methodik für das Testen von Anwendungen vor ihrem erstmaligen Einsatz und nach wesentlichen Änderungen zu definieren und einzuführen. Die Tests haben in ihrem Umfang die Funktionalität der Anwendung und die Sicherheitskontrollenimplementierten Maßnahmen zum Schutz der Informationen einzubeziehen. Sofern bei einer Anwendung die Systemleistung von Bedeutung ist, ist auch diese unter verschiedenen, sachgerechten Stressbelastungsszenarien zu testen. Die fachlich zuständigen Stellen haben die Durchführung von fachlichen Abnahmetests verantwortet der für die Anwendung zuständige Fachbereichzu verantworten. Testumgebungen zur Durchführung der Abnahmetests haben in für den Test wesentlichen Aspekten der Produktionsumgebung zu entsprechen. Testaktivitäten und Testergebnisse sind zu dokumentieren.	Dies umfasst eineDie Testdurchführung erfordert einschlägige Expertise der für den Test verantwortlichen Personen sowie eine angemessen ausgestaltete Unabhängigkeit von den Anwendungsentwicklern. Der Schutzbedarf der zum Test verwendeten Daten ist zu berücksichtigen. Eine Testdokumentation enthält mindestens folgende Punkte: ■ Testfallbeschreibung, ■ Dokumentation der zugrunde gelegten Parametrisierung des Testfalls, ■ Testdaten, ■ erwartetes Testergebnis, ■ erzieltes Testergebnis, ■ aus den Tests abgeleitete Maßnahmen. Sofern der Schutz der Informationen dies erfordert, sind Penetrationstests in die Testaktivitäten mit einzubeziehen.
6.14.7.14. Nach Produktivsetzung dereiner Anwendung sind mögliche Abweichungen vom Regelbetrieb angemessen zu überwachen, deren Ursachen zu untersuchen und ggf. Maßnahmen zur Nachbesserung zu veranlassen.	Nach der Produktivsetzung bedarf es einer temporär erhöhten Überwachung. Hinweise auf erhebliche Mängel können z. B. Häufungen der Abweichungen vom Regelbetrieb sein.
6.15.7.15. Ein angemessenes Verfahren für die Klassifizierung/Kategorisierung (Schutzbedarfsklasse) und den Umgang mit den von Endbenutzern Mitarbeitern des Fachbereichs entwickelten oder betriebenen Anwendungen (IDV) ist festzulegen.	Die Einhaltung von ProgrammierstandardsProgrammierrichtlinien wird auch für die von Endbenutzern in den Fachbereichen entwickelten IDV-Anwendungen (z. B. IDV-Anwendung) sichergestellt. Jede dieser AnwendungenAnwendung wird einer Schutzbedarfsklasse zugeordnet. Übersteigt der ermit-

telte Schutzbedarf die technische Schutzmöglichkeit ~~dieser Anwendungen~~einer Anwendung, werden Schutzmaßnahmen in Abhängigkeit der Ergebnisse der Schutzbedarfsklassifizierung ergriffen.

~~6.16.~~7.16. Die Vorgaben zur Identifizierung der von ~~Endbenutzern~~Mitarbeitern des Fachbereichs entwickelten oder betriebenen Anwendungen, zur Dokumentation, zu den Programmierrichtlinien und zur Methodik des Testens dieser Anwendungen, zur Schutzbedarfsfeststellung und zum Rezertifizierungsprozess der Berechtigungen sind zu regeln (z. B. in einer IDV-Richtlinie).

Für einen Überblick und zur Vermeidung von Redundanzen wird ein zentrales Register der kritischen bzw. wesentlichen Anwendungen geführt. Das Register beinhaltet grundsätzlich zumindest die Anwendungen, die zur Identifizierung, Bewertung, Überwachung und Steuerung der Risiken sowie zur Berichterstattung über diese Risiken eingesetzt werden oder die für die Durchführung anderer, aufgrund gesetzlicher Vorgaben oder für den Betrieb notwendiger Tätigkeiten, von Bedeutung sind.

Es werden mindestens folgende Informationen erhoben:

- Name und Zweck der Anwendung,
- Versionierung, Datumsangabe,
- Fremd- oder Eigenentwicklung,
- Fachverantwortliche(r) Mitarbeiter,
- ~~Technisch~~technisch verantwortliche(r) Mitarbeiter,
- Technologie,
- Ergebnis der Risikoklassifizierung/Schutzbedarfseinstufung und ggf. die daraus abgeleiteten Schutzmaßnahmen.

~~7.~~8. IT-Betrieb ~~(inkl. Datensicherung)~~

~~7.1.~~8.1. Der IT-Betrieb hat die ~~Erfüllung der~~ Anforderungen, die sich aus der Umsetzung der Geschäftsstrategie sowie aus den IT-unterstützten Geschäftsprozessen ergeben (vgl. ~~II. Rn. 14 und 15), umzusetzen.~~Kap. 2.9 und 2.10), zu erfüllen.

~~7.2.~~8.2. Die Komponenten der IT-Systeme ~~sowie~~und deren Beziehungen zueinander sind in geeigneter Weise zu verwalten~~,~~ und die hierzu erfassten Bestandsangaben sind regelmäßig sowie anlassbezogen zu aktualisieren.

Zu den Bestandsangaben zählen insbesondere:

- Bestand und Verwendungszweck der Komponenten der IT-Systeme mit den relevanten Konfigurationsangaben~~,~~ (z. B. Versionen und Patchlevel),
- Eigentümer der IT-Systeme und deren Komponenten,
- Standort der Komponenten der IT-Systeme,
- Aufstellung der relevanten Angaben zu Gewährleistungen und sonstigen Supportverträgen (ggf. Verlinkung),
- Angaben zum Ablaufdatum des Supportzeitraums der Komponenten der IT-Systeme,
- ~~Akzeptierter~~Schutzbedarf und Kritikalitätseinstufung der IT-Systeme und deren Komponenten,
- akzeptierter Zeitraum der Nichtverfügbarkeit der IT-Systeme sowie der maximal tolerierbare Datenverlust.

~~7.3.~~8.3. Das Portfolio aus IT-Systemen ~~ist angemessen zu steuern. Hierbei~~bedarf der Steuerung. IT-Systeme sollten regelmäßig aktualisiert werden ~~auch die~~. Risiken aus veralteten bzw. nicht mehr vom Hersteller unterstützten IT-Systemen ~~berücksichtigt (Lebens-Zyklus~~ sind zu steuern (Lebenszyklus-Management). Nicht mehr verwendete Hardwarekomponenten sind sicher zu entsorgen.

Zu den Hardwarekomponenten zählen insbesondere Datenträger.

~~7.4.~~8.4. Die Prozesse zur Änderung von IT-Systemen sind abhängig vom Risikoprofil auszugestalten und umzusetzen. Dies gilt ~~ebenso~~auch für Neu- oder Ersatzbeschaffungen von IT-Systemen sowie für sicherheitsrelevante Nachbesserungen (Sicherheitspatches).	Änderungen von IT-Systemen umfassen auch die Wartung von IT-Systemen. Beispiele für Änderungen sind: ■ Funktionserweiterungen oder Fehlerbehebungen von ~~Software-Komponenten~~Softwarekomponenten, ■ Datenmigrationen, ■ Änderungen an Konfigurationseinstellungen von IT-Systemen, ■ Austausch von ~~Hardware-Komponenten~~Hardwarekomponenten (Server, Router etc.), ■ Einsatz neuer ~~Hardware-Komponenten~~Hardwarekomponenten, ■ Umzug der IT-Systeme zu einem anderen Standort.
~~7.5.~~8.5. ~~Anträge zur~~ Änderung von IT-Systemen und größere Prozessänderungen mit Auswirkungen auf die Informationssicherheit sind zu beantragen. Die Anträge sind in geordneter Art und Weise aufzunehmen, zu dokumentieren, unter Berücksichtigung möglicher Umsetzungsrisiken zu bewerten, zu priorisieren und zu genehmigen. Die Änderung ist koordiniert und sicher umzusetzen. Auch für zeitkritische Änderungen von IT-Systemen sind geeignete Prozesse einzurichten.	Der sicheren Umsetzung der Änderungen in den produktiven Betrieb dienen beispielsweise: ■ Risikoanalyse in Bezug auf die bestehenden IT-Systeme (insbesondere auch das Netzwerk und die vor- und nachgelagerten IT-Systeme), auch im Hinblick auf mögliche Sicherheits- oder Kompatibilitätsprobleme, als Bestandteil der Änderungsanforderung, ■ Tests von Änderungen vor Produktivsetzung auf mögliche Inkompatibilitäten der Änderungen sowie mögliche sicherheitskritische Aspekte bei ~~maßgeblichen~~ bestehenden IT-Systemen, ■ Tests von Patches vor Produktivsetzung unter Berücksichtigung ihrer Kritikalität, ■ Datensicherungen der betroffenen IT-Systeme,

- Rückabwicklungspläne, um eine frühere Version des IT-Systems wiederherstellen zu können, wenn während oder nach der Produktivsetzung ein Problem auftritt,
- alternative Wiederherstellungsoptionen, um dem Fehlschlagen primärer Rückabwicklungspläne begegnen zu können.

Für risikoarme Konfigurationsänderungen/Parametereinstellungen (z. B. Änderungen am Layout von Anwendungen, Austausch von defekten Hardwarekomponenten, Zuschaltung von Prozessoren) können abweichende prozessuale Vorgaben/Kontrollen definiert werden (z. B. Vier-Augen-Prinzip, Dokumentation der Änderungen oder der nachgelagerten Kontrolle).

~~7.6.~~8.6. Die Meldungen über ungeplante Abweichungen vom Regelbetrieb (Störungen) und deren Ursachen sind in geeigneter Weise zu erfassen, zu bewerten, insbesondere hinsichtlich möglicherweise resultierender Risiken zu priorisieren und entsprechend festgelegter Kriterien zu eskalieren. Hierzu sind Standardvorgehensweisen z. B. für Maßnahmen und Kommunikation sowie Zuständigkeiten (z. B. für Schadcode auf Endgeräten, Fehlfunktionen) zu definieren. Bearbeitung, Ursachenanalyse und Lösungsfindung inkl. Nachverfolgung sind zu dokumentieren. Ein geordneter Prozess zur Analyse möglicher Korrelationen von Störungen und deren Ursachen muss vorhanden sein. Der Bearbeitungsstand offener Meldungen über Störungen sowie die Angemessenheit der Bewertung und Priorisierung, sind zu überwachen und zu steuern. Das Unternehmen hat geeignete Kriterien für die Information der Beteiligten (z. B. Geschäftsleitung, zuständige Aufsichtsbehörde) über Störungen festzulegen.

Die Identifikation der Risiken kann beispielsweise anhand des Aufzeigens der Verletzung der Schutzziele erfolgen.

Die Ursachenanalyse erfolgt auch dann, wenn mehrere IT-Systeme zur Störungs- und Ursachenerfassung sowie -bearbeitung eingesetzt werden.

~~7.7.~~8.7. Die Vorgaben für die Verfahren zur Datensicherung (ohne Datenarchivierung) sind schriftlich in einem Datensicherungskonzept zu regeln. Die im Datensicherungskonzept dargestellten Anforderungen an die Verfügbarkeit, Lesbarkeit und Aktualität der Kunden- und Geschäftsdaten sowie an die für deren Verarbeitung notwendigen IT-Systeme sind aus den Anforderungen der Geschäftsprozesse und den Geschäftsfortführungsplänen abzuleiten. Die Verfahren zur ~~Wiederherstellbarkeit im erforderlichen Zeitraum~~Wiederherstellung und zur Gewährleistung der Lesbarkeit ~~von Datensicherungen~~der Daten sind regelmäßig, mindestens jährlich, im Rahmen einer Stichprobe sowie anlassbezogen zu testen.

Die Anforderungen an die ~~Ausgestaltung~~Maßnahmen zur Sicherstellung von Verfügbarkeit, Lesbarkeit und ~~Lagerung~~Aktualität der ~~Datensicherungen~~Daten sowie an die durchzuführenden Tests ergeben sich aus diesbezüglichen Risikoanalysen. Hinsichtlich der Standorte für die Lagerung der Datensicherungen können eine oder mehrere weitere Lokationen erforderlich sein.

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.

~~8.~~9. Ausgliederungen von IT-Dienstleistungen und sonstige Dienstleistungsbeziehungen im Bereich IT-Dienstleistungen~~; isolierter Bezug von Hard- und/oder Software~~

~~8.1.~~9.1. Bei Ausgliederungen von IT-Dienstleistungen - unabhängig davon, ob es sich hierbei um die Hauptdienstleistung oder um eine ergänzende Nebendienstleistung zu einer anderen Hauptdienstleistung handelt - sind die hierfür jeweils geltenden Anforderungen zu erfüllen; insbesondere ist vorab eine Risikoanalyse durchzuführen. Dies gilt auch für Ausgliederungen von solchen IT-Dienstleistungen, die dem Unternehmen durch ein Dienstleis-

tungsunternehmen über ein Netz bereitgestellt werden (z. B. Rechenleistung, Speicherplatz, Plattformen oder Software) und deren Angebot, Nutzung und Abrechnung dynamisch und an den Bedarf angepasst über definierte technische Schnittstellen sowie Protokolle erfolgen (Cloud-Dienstleistungen).

~~8.2.~~9.2. Das Unternehmen hat auch in Bezug auf jede sonstige Dienstleistungsbeziehung im Bereich der IT-Dienstleistungen - unabhängig davon, ob es sich hierbei um die Hauptdienstleistung oder um eine ergänzende Nebendienstleistung zu einer anderen Hauptdienstleistung handelt - vorab eine Erhebung und Bewertung der Anforderungen sowie eine Risikoanalyse durchzuführen.	Art und Umfang einer Risikoanalyse kann das Unternehmen unter Proportionalitätsgesichtspunkten festlegen. Für gleichartige sonstige Dienstleistungsbeziehungen im Bereich der IT-Dienstleistungen kann auf bestehende Risikoanalysen zurückgegriffen werden. Die für Informationssicherheit und Notfallmanagement verantwortlichen Funktionen oder Personen des Unternehmens werden in die Risikoanalyse eingebunden.
~~8.3.~~9.3. Sonstige Dienstleistungsbeziehungen im Bereich der IT-Dienstleistungen sind im Einklang mit den Strategien unter Berücksichtigung der Risikoanalyse des Unternehmens zu steuern. Die Erbringung der vom Dienstleister geschuldeten Leistung ist entsprechend der Risikoanalyse zu überwachen.	Hierfür wird eine vollständige, strukturierte Vertragsübersicht vorgehalten. Die Steuerung kann auf der Basis dieser Vertragsübersicht durch Bündelung von Verträgen über sonstige Dienstleistungsbeziehungen im Bereich der IT-Dienstleistungen (Vertragsportfolio) erfolgen. Bestehende Steuerungsmechanismen können hierzu genutzt werden.
~~8.4.~~9.4. Die aus der Risikoanalyse in Bezug auf sonstige Dienstleistungsbeziehungen im Bereich der IT-Dienstleistungen abgeleiteten Maßnahmen sind angemessen in der Vertragsgestaltung zu berücksichtigen. Die Ergebnisse der Risikoanalyse sind in angemessener Art und Weise im Managementprozess des operationellen Risikos, vor allem im Bereich der Gesamtrisikobewertung des operationellen Risikos, zu berücksichtigen.	Dies beinhaltet beispielsweise Vereinbarungen zum Informationsrisikomanagement, zum Informationssicherheitsmanagement ~~und~~, zum Notfallmanagement und zum IT-Betrieb, die im Regelfall den Zielvorgaben des Unternehmens entsprechen. (z. B. Informationssicherheitsleit- und -richtlinie). Bei Relevanz wird auch die Möglichkeit eines Ausfalls eines IT-Dienstleisters berücksichtigt und eine diesbezügliche Exit- oder Alternativ-Strategie entwickelt und dokumentiert.

	Als erforderlich erkannte Maßnahmen sind auch im Fall der Einbindung von Subunternehmen des IT-Dienstleisters zu berücksichtigen.
~~8.5.~~9.5. Die Risikoanalysen in Bezug auf sonstige Dienstleistungsbeziehungen im Bereich der IT-Dienstleistungen sind bei wesentlichen Änderungen des Risikoprofils erneut durchzuführen und ggf. die Vertragsinhalte anzupassen.	
~~8.6.~~9.6. ~~II. Rn. 66~~Kap. 9.2 bis ~~69~~9.5 gelten auch für den isolierten Bezug von Hard- und/oder Software.	Der isolierte Bezug von Hard- und/oder Software durch das Unternehmen ist nicht als Ausgliederung einzustufen. Unterstützungsleistungen wie beispielsweise ■ die Anpassung der Software an die Erfordernisse des Unternehmens, ■ die entwicklungstechnische Umsetzung von Änderungswünschen (Programmierung), ■ das Testen, die Freigabe und die Implementierung der Software in die Produktionsprozesse beim erstmaligen Einsatz und bei wesentlichen Veränderungen, insbesondere von programmtechnischen Vorgaben, ■ Fehlerbehebungen gemäß der Anforderungs-/Fehlerbeschreibung des Auftraggebers oder Herstellers, ■ sonstige Unterstützungsleistungen, die über die reine Beratung hinausgehen, sind in der Regel als Ausgliederung einzustufen, wenn sie sich auf Software beziehen, die zur Identifizierung, Bewertung, Überwachung und Steuerung der Risiken sowie zur Berichterstattung über diese Risiken eingesetzt wird oder die für die Durchführung anderer aufgrund gesetzlicher Vorgaben oder für den Betrieb notwendiger Tätigkeiten von Bedeutung ist. Auch auf diese

Unterstützungsleistungen finden die jeweils geltenden Anforderungen an Ausgliederungen Anwendung.

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.

Das IT-Notfallkonzept hat mindestens folgende Szenarien 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, Lebensmittelvergiftung, 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 (vgl. Kap. 3.5) 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	Das Testkonzept beinhaltet mindestens sowohl Tests einzelner IT-Systeme (z. B. Komponenten, einzelne Anwendungen) als auch deren Zusammenfassung zu Systemverbünden.

schriftlich zu dokumentieren. Resultierende Mängel sind zu analysieren und an die Geschäftsleitung zu berichten.

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.

~~9.~~11. Kritische Infrastrukturen

~~9.1.~~11.1. Dieses ~~Modul~~Kapitel richtet sich - im Kontext mit den anderen ~~Modulen~~Kapiteln der VAIT und den sonstigen einschlägigen versicherungsaufsichtlichen Anforderungen in Bezug auf die Sicherstellung angemessener Vorkehrungen zur Gewährleistung von Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Informationsverarbeitung - eigens an die Betreiber kritischer Infrastrukturen (KRITIS-Betreiber[2]).

Es ergänzt insoweit die versicherungsaufsichtlichen Anforderungen an die IT um Anforderungen an die wirksame Umsetzung besonderer Maßnahmen zum Erreichen des KRITIS-Schutzziels. Als KRITIS-Schutzziel wird das Bewahren der Versorgungssicherheit der Gesellschaft mit den in § 7 BSI-Kritisverordnung genannten kritischen Versicherungsdienstleistungen verstanden, da deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen könnte.

Für kritische Dienstleistungen sind von den jeweiligen KRITIS-Betreibern (und im Falle von Ausgliederungen zusätzlich von ihren IT-Dienstleistern) geeignete Maßnahmen zu beschreiben und wirksam umzusetzen, die die Risiken für den sicheren Betrieb kritischer Infrastrukturen auf ein dem KRITIS-Schutzziel angemessenes Niveau senken. Hierzu müssen sich die KRITIS-Betreiber sowie ihre IT-Dienstleister an den einschlägigen Standards orientieren. Dabei soll der Stand der Technik eingehalten werden.

[2] Siehe Erste Verordnung zur Änderung der BSI-Kritisverordnung vom 21. Juni 2017

Dieses ~~Modul~~Kapitel kann verwendet werden, um durch Sicherheitsaudits oder Prüfungen (beispielsweise im Rahmen der Jahresabschlussprüfung) den Nachweis nach § 8a Abs. 3 BSIG zu erbringen. Dazu müssen die Anforderungen der VAIT für alle informationstechnischen Systeme, Komponenten oder Prozesse der kritischen Infrastrukturen umgesetzt und in der Prüfung komplett abgedeckt sein. Der Nachweis gemäß § 8a Abs. 3 BSIG ist unter Hinzuziehung einer geeigneten prüfenden Stelle (siehe einschlägige FAQ auf der BSI-Website) zu erstellen.

Alternativ können die KRITIS-Betreiber für den Nachweis gemäß § 8a Abs. 3 BSIG einen unternehmensindividuellen Ansatz unter Berücksichtigung anderer geeigneter Anforderungen verfolgen oder einen branchenspezifischen Sicherheitsstandard (B3S) gemäß § 8a Abs. 2 BSIG erstellen.

~~9.2.~~11.2. Der Geltungsbereich für die Nachweiserbringung für die kritische Infrastruktur muss die Anlage gemäß BSI-KritisV vollständig umfassen. Dies ist innerhalb des Informationsverbundes eindeutig zu kennzeichnen. Hierbei sind alle relevanten Schnittstellen einzubeziehen.

Alle einschlägigen Anforderungen der VAIT und der sonstigen aufsichtlichen Anforderungen sind nachvollziehbar auch auf alle Komponenten und Bereiche der kritischen Dienstleistung anzuwenden.

Kritische Dienstleistungen sind angemessen zu überwachen. Mögliche Auswirkungen von Sicherheitsvorfällen auch auf die kritischen Dienstleistungen sind zu bewerten.

Dies kann beispielsweise erfolgen, indem in den Bestandsangaben entsprechend ~~Rn. 59~~Kap. 8.2 VAIT (beispielsweise in einer Configuration~~-~~-Management~~-~~-Database – CMDB) die Komponenten und Bereiche des Informationsverbundes zusätzlich gekennzeichnet werden, die zu den kritischen Infrastrukturen gehören. Der Bezug zu den jeweiligen zu prüfenden Anlagenkategorien des KRITIS-Betreibers ist darzustellen.

Durch geeignete Maßnahmen ist sicherzustellen, dass die für die kritischen Dienstleistungen betriebsrelevanten Systeme einer resilienten Architektur unterliegen.

~~9.3.~~11.3. Im Rahmen des Informationsrisiko- und Informationssicherheits-managements gemäß den VAIT-~~Modulen 3~~Kapiteln 3 und ~~4~~4 ist das KRITIS-Schutzziel zu beachten und Maßnahmen zu dessen Einhaltung wirksam umzusetzen. Insbesondere sind Risiken, die die kritischen Dienstleistungen in relevantem Maße beeinträchtigen können, durch angemessene Maßnahmen der Risikominderung oder -vermeidung auf ein dem KRITIS-Schutzziel angemessenes Niveau zu senken.

Grundsätzlich sind für Risiken geeignete Maßnahmen zur Mitigation zu treffen. Dabei soll der Stand der Technik eingehalten werden.

Hierbei ist allerdings die Angemessenheit zu wahren: Der erforderliche Aufwand soll im Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur stehen. Dies bedeutet, dass Risiken zwar auch akzeptiert oder übertragen werden können, dies aber nicht allein nach betriebswirtschaftlichen Gesichtspunkten entschieden werden darf, sondern nur unter Gewährleistung der Versorgungssicherheit. Risiken,

	Hierzu sind insbesondere solche Maßnahmen geeignet, mit denen den Risiken für die Verfügbarkeit bei einem hohen und sehr hohen Schutzbedarf begegnet werden kann.	die die kritische Dienstleistung betreffen, dürfen beispielsweise nicht akzeptiert werden, sofern Vorkehrungen nach dem Stand der Technik möglich und angemessen sind. Auch ein Transfer der Risiken, z. B. durch Versicherungen, ist kein Ersatz für angemessene Vorkehrungen. Der Abschluss einer Versicherung, z. B. aus betriebswirtschaftlichem Interesse, steht dem nicht entgegen.
~~9.4.~~11.4.	Das KRITIS-Schutzziel ist von der Schutzbedarfsermittlung über die Definition angemessener Maßnahmen bis hin zur wirksamen Umsetzung dieser Maßnahmen einschließlich der Implementierung und des regelmäßigen Testens entsprechender Notfallvorsorgemaßnahmen stets mit zu berücksichtigen.	Insbesondere ist dies bei den folgenden Aspekten zu beachten: Das KRITIS-Schutzziel ist auch bei Ausgliederungen von Dienstleistungen entsprechend §§ 7 Nr. 2 und 32 VAG i. V. m. ~~Modul 8~~ Kapitel 9 VAIT zu berücksichtigen. Im Rahmen der Notfallvorsorge sind Maßnahmen zu ergreifen, mit denen die kritischen Dienstleistungen auch im Notfall aufrechterhalten werden können.
~~9.5.~~11.5.	Die Nachweiserbringung gemäß § 8a Abs. 3 BSIG bzgl. der Einhaltung der Anforderungen gemäß § 8a Abs. 1 BSIG kann durch Sicherheitsaudits oder Prüfungen (beispielsweise im Rahmen der Jahresabschlussprüfung) erfolgen. Der KRITIS-Betreiber hat die einschlägigen Nachweisdokumente fristgerecht beim BSI einzureichen, entsprechend den jeweils gültigen Vorgaben des BSI.	Neben Sicherheitsaudits oder Prüfungen (beispielsweise im Rahmen der Jahresabschlussprüfung) auf Basis der VAIT sind weitere Möglichkeiten zur Nachweiserbringung zulässig. Die KRITIS-Betreiber sollten entsprechend die „Orientierungshilfe zu Nachweisen gemäß § 8a Abs. 3 BSIG“ in der jeweils aktuellen Fassung beachten. Die Nachweiserbringung über die Einhaltung der Anforderungen gemäß § 8a Abs. 1 BSIG erfolgt durch den KRITIS-Betreiber erstmals bis spätestens zum 30.06.2019 und ist anschließend mindestens alle zwei Jahre gegenüber dem BSI durchzuführen.