BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

# Versicherungsaufsichtliche Anforderungen an die IT (VAIT)

Rundschreiben 10/2018 (VA) in der Fassung vom 20.03.2019

BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

# Inhalt

# 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 Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) enthaltenen Anforderungen unberührt und werden im Rahmen ihres Gegenstandes durch dieses Rundschreiben konkretisiert.

5 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 (Hard-

ware- 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 ISO/IEC 2700X der International Organization for Standardization.

6 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). 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 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 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 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.

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

11 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 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 regelmäßig und anlassbezogen zu überprüfen und erforderlichenfalls anzupassen. Die Geschäftsleitung muss für die Umsetzung der IT-Strategie Sorge tragen.

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 sowie zum isolierten Bezug von Hard- und/oder Software (zusammen auch „Bezug von IT“);
(b) Zuordnung der gängigen Standards, auf die das Unternehmen abstellt, auf die Bereiche der IT;
(c) Zuständigkeiten und Einbindung der Informationssicherheit in die Organisation;
(d) strategische Entwicklung der IT-Architektur;
(e) Aussagen zum Notfallmanagement unter Berücksichtigung der IT-Belange;
(f) Aussagen zu den in den Fachbereichen selbst betriebenen und entwickelten IT-Systemen.

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;

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;

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.

3 Die in der IT-Strategie niedergelegten Ziele sind so zu formulieren, dass eine sinnvolle Überprüfung der Zielerreichung möglich ist.

| | | |
|---|---|---|
| 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. |
| 5 | Die Inhalte sowie Änderungen der IT-Strategie sind innerhalb des Unternehmens in geeigneter Weise zu kommunizieren. | |

## 2. IT-Governance

| | | |
|---|---|---|
| 6 | 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 der IT sowie zum Umfang und zur Qualität der technisch-organisatorischen Ausstattung. Die Regelungen für die IT-Aufbau- und IT-Ablauforganisation sind bei Veränderungen der Aktivitäten und Prozesse zeitnah anzupassen. | |
| 7 | Die Geschäftsleitung ist dafür verantwortlich, dass auf Basis der IT-Strategie die Regelungen zur IT-Aufbau- und IT-Ablauforganisation festgelegt und bei Veränderungen der Aktivitäten und Prozesse zeitnah angepasst werden. Diese Regelungen 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 wirksam umgesetzt werden. Dies gilt auch bezüglich der Schnittstellen zu wichtigen Ausgliederungen. | Die Geschäftsleitung hat den Regelungen zur IT-Aufbau- und IT-Ablauforganisation zumindest bei Erstverabschiedung sowie bei nicht geringfügigen Änderungen zuzustimmen. Sollen geringfügige Änderungen vom Zustimmungserfordernis ausgenommen werden, hat das Unternehmen im Vorfeld festzulegen, welche Änderungen als geringfügig einzuschätzen sind. |
| 8 | 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. | |
| 9 | Das Unternehmen hat insbesondere das Informationsrisikomanagement, das Informationssicherheitsmanagement, den IT-Betrieb und die Anwendungsentwicklung quantitativ und qualitativ angemessen mit Personal auszustatten. | Hinsichtlich der Maßnahmen zur Erhaltung einer angemessenen qualitativen Personalausstattung werden insbesondere der Stand der Technik sowie die aktuelle und zukünftige Entwicklung der Bedrohungslage berücksichtigt. |
| 10 | 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. |

| | | |
|---|---|---|
| 11 | Die Abwesenheit oder das Ausscheiden von Mitarbeitern darf nicht zu nachhaltigen Störungen der Betriebsabläufe führen. | |
| 12 | 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.<br><br>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. |
| 13 | Zur Steuerung der für den Betrieb und die Weiterentwicklung der IT-Systeme zuständigen Bereiche durch die Geschäftsleitung sind angemessene quantitative oder qualitative Kriterien festzulegen, und deren Einhaltung ist zu überwachen. | Bei der Festlegung der Kriterien können z. B. die Qualität der Leistungserbringungen, die Verfügbarkeit, Wartbarkeit, Anpassbarkeit an neue Anforderungen, Sicherheit der IT-Systeme oder der dazugehörigen IT-Prozesse sowie deren Kosten berücksichtigt werden. |
| 14 | Umfang und Qualität der technisch-organisatorischen Ausstattung haben sich am Risikoprofil zu orientieren. | |
| 15 | 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 Tätigkeit benötigt; 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. | |
| 16 | Das Unternehmen hat sicherzustellen, dass die IT-bezogenen Geschäftsaktivitäten auf der Grundlage von Arbeitsablaufbeschreibungen (Organisationsrichtlinien) betrieben | Hinsichtlich der Darstellung der Organisationsrichtlinien kommt es in erster Linie darauf an, dass diese sachgerecht und für die Mitarbeiter des Unternehmens nachvollziehbar |

werden. Der Detaillierungsgrad der Organisationsrichtlinien hängt vom Risikoprofil ab.

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

| | | |
|---|---|---|
| 17 | 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. | |
| 18 | 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. | |
| 19 | 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 sind. |
| 20 | 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, IT-Systeme sowie Netz- und Gebäudeinfrastrukturen. |
| 21 | Die Methodik zur Ermittlung des Schutzbedarfs (insbesondere im Hinblick auf die Schutzziele „Integrität“, „Verfügbarkeit“, „Vertraulichkeit“ und „Authentizität") hat die Konsistenz der resultierenden Schutzbedarfe nachvollziehbar sicherzustellen. | Schutzbedarfskategorien sind beispielhaft „Niedrig“, „Mittel“, „Hoch“ und „Sehr hoch“. |
| 22 | Die Anforderungen des Unternehmens zur Umsetzung der Schutzziele in den Schutzbedarfskategorien sind durch das Unternehmen festzulegen und in geeigneter Form zu dokumentieren (Sollmaßnahmenkatalog). | Der Sollmaßnahmenkatalog enthält lediglich die Anforderung, nicht jedoch deren konkrete Umsetzung. |

| | | |
|---|---|---|
| 23 | Auf Basis der festgelegten IT-Risikokriterien hat eine Risikoanalyse zu erfolgen. 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. | IT-Risikokriterien enthalten beispielsweise mögliche Bedrohungen, das Schadenspotenzial, die Schadenshäufigkeit sowie den Risikoappetit.<br><br>Die Risikoanalyse kann u. a. auch auf Grundlage eines Vergleichs der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen erfolgen. |
| 24 | 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. |

## 4. Informationssicherheitsmanagement

25 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.

26 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.

In der Informationssicherheitsleitlinie werden die Ziele und der Geltungsbereich für die Informationssicherheit festgelegt und die wesentlichen organisatorischen Aspekte des Informationssicherheitsmanagements beschrieben. Regelmäßige Überprüfungen und Anpassungen an geänderte Bedingungen werden risikoorientiert vorgenommen. Veränderungen der IT-Aufbau- und IT-Ablauforganisation sowie der IT-Systeme einer Institution (Geschäftsprozesse, Fachaufgaben, organisatorische Gliederung) werden hierbei ebenso berücksichtigt wie Veränderungen der äußeren Rahmenbedingungen (z. B. gesetzliche Regelungen, regulatorische Anforderungen), der Bedrohungsszenarien oder der Sicherheitstechnologien.

27 Auf Basis der Informationssicherheitsleitlinie sind konkretisierende, den Stand der Technik berücksichtigende Informationssicherheitsrichtlinien und Informationssicherheitsprozesse mit den Teilprozessen Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung zu definieren.

Informationssicherheitsrichtlinien werden beispielsweise für die Bereiche Netzwerksicherheit, Kryptografie, Authentisierung und Protokollierung erstellt.

Informationssicherheitsprozesse dienen in erster Linie der Erreichung der vereinbarten Schutzziele. Dazu gehört u. a., Informationssicherheitsvorfällen vorzubeugen und diese zu identifizieren sowie die angemessene Reaktion und Kommunikation im weiteren Verlauf.

28 Das Unternehmen 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 Ziele und Maßnahmen hinsichtlich der Informationssicherheit sowohl intern als auch - sofern und soweit geboten - gegenüber Dritten transparent gemacht und deren Einhaltung 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,
- Beteiligung bei der Erstellung und Fortschreibung des Notfallkonzepts bzgl. der IT-Belange,
- 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),
- 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.

29 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,
- Festlegung der erforderlichen Ressourcenausstattung für die Funktion des Informationssicherheitsbeauftragten,
- ein der Funktion zugewiesenes Budget für Informationssicherheits-schulungen im Unternehmen und die persönliche Weiterbildung des Informationssicherheitsbeauftragten,
- 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 Sachverhalte, die das Unternehmen betreffen.<br>■ 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.<br>■ Der Informationssicherheitsbeauftragte nimmt keine Aufgaben der internen Revision wahr. |
| 30 | 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.<br><br>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. |
| 31 | Nach einem Informationssicherheitsvorfall sind die Auswirkungen auf die Informationssicherheit zu analysieren und angemessene Nachsorgemaßnahmen zu veranlassen. | Die Definition des Begriffes „Informationssicherheitsvorfall“ nach Art und Umfang basiert auf dem Schutzbedarf der betroffenen Geschäftsprozesse, IT-Systeme und den zugehörigen IT-Prozessen. 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 „Informationssicherheitsvorfall“ ist nachvollziehbar vom Begriff „Abweichung vom Regelbetrieb“ (im Sinne von „Störung im Tagesbetrieb“) abzugrenzen. |
| 32 | Der Informationssicherheitsbeauftragte hat der Geschäftsleitung, ggf. dem zuständigen Geschäftsleiter, regelmäßig, mindestens vierteljährlich, und ggf. ad hoc, über den Status der Informationssicherheit zu berichten. | Der Statusbericht enthält beispielsweise die Bewertung der Informationssicherheitslage im Vergleich zum Vorbericht, Informationen zu Projekten zur Informationssicherheit, Informationssicherheitsvorfälle sowie Penetrationstest-Ergebnisse. |

## 5. Benutzerberechtigungsmanagement

33 Das Unternehmen hat ein Benutzerberechtigungsmanagement 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 sind die Anforderungen an die Ausgestaltung der Prozesse (siehe II. Rn. 7 und 15) entsprechend zu berücksichtigen.

34 Im Rahmen des Benutzerberechtigungsmanagements legen Berechtigungskonzepte den Umfang und die Nutzungsbedingungen der Berechtigungen für die IT-Systeme konsistent zum ermittelten Schutzbedarf sowie vollständig und nachvollziehbar ableitbar für alle von einem IT-System bereitgestellten Berechtigungen fest. Berechtigungskonzepte haben im Hinblick auf die Vergabe von Berechtigungen an Benutzer 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 zu wahren und Interessenskonflikte des Personals zu vermeiden. Bei IT-gestützter Bearbeitung ist die Funktionstrennung durch entsprechende Verfahren und Schutzmaßnahmen sicherzustellen.

Eine mögliche Nutzungsbedingung ist die Befristung der eingeräumten Berechtigungen. Berechtigungen können sowohl für personalisierte, für nicht personalisierte als auch für technische Benutzer vorliegen.

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.

35 Nicht personalisierte Berechtigungen müssen jederzeit zweifelsfrei einer handelnden natürlichen Person (möglichst automatisiert) zuzuordnen sein. Abweichungen in begründeten Ausnahmefällen und die hieraus resultierenden Risiken sind zu genehmigen und zu dokumentieren.

36 Jeder technische Benutzer muss einer verantwortlichen natürlichen Person zugeordnet sein.

37 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 Umsetzung des Berechtigungsantrags im Zielsystem.

| | | |
|---|---|---|
| | | Bei Einrichtung und Änderung von Berechtigungen bedarf es der vorherigen Zustimmung der fachlich verantwortlichen Stelle, bei Deaktivierung oder Löschung ist sie zeitnah zu informieren. |
| 38 | 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).<br><br>Bei der Rezertifizierung sind die für die Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen zuständigen Kontrollinstanzen mit einzubeziehen. | 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.<br><br>Fällt im Rahmen der Rezertifizierung auf, dass außerhalb des vorgeschriebenen Verfahrens Berechtigungen eingeräumt wurden, so werden diese gemäß der Regelverfahren zur Einrichtung, Änderung und Löschung von Berechtigungen entzogen. |
| 39 | Die Einrichtung, Änderung, Deaktivierung sowie Löschung von Berechtigungen und die Rezertifizierung sind nachvollziehbar und auswertbar zu dokumentieren. | |
| 40 | Das Unternehmen 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. | 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. |
| 41 | Durch begleitende technisch-organisatorische Maßnahmen ist einer Umgehung der Vorgaben der Berechtigungskonzepte vorzubeugen. | Technisch-organisatorische Maßnahmen hierzu sind beispielsweise:<br><br>■ Auswahl angemessener Authentifizierungsverfahren,<br>■ Implementierung einer Richtlinie zur Wahl sicherer Passwörter,<br>■ automatischer passwortgesicherter Bildschirmschoner,<br>■ Verschlüsselung von Daten,<br>■ eine manipulationssichere Implementierung der Protokollierung,<br>■ Maßnahmen zur Sensibilisierung der Mitarbeiter. |

## 6. IT-Projekte, Anwendungsentwicklung (inkl. durch Endbenutzer in den Fachbereichen)

42 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 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.

43 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 sind dabei grundsätzlich voneinander 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.

44 Die Anforderungen unter II. Rn. 14, 15, 18 und 43 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.

45 Die organisatorischen Grundlagen von IT-Projekten (inkl. Qualitätssicherungsmaßnahmen) 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.

46 IT-Projekte sind angemessen zu steuern, insbesondere unter Berücksichtigung der Risiken im Hinblick auf die Dauer, den Ressourcenverbrauch und ihre Qualität. Hierfür sind Vorgehensmodelle festzulegen, deren Einhaltung zu überwachen ist.

Beispielsweise kann die Entscheidung über den Übergang zwischen den Projektphasen von eindeutigen Qualitätskriterien des jeweiligen Vorgehensmodells abhängen.

| | | |
|---|---|---|
| 47 | 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. |
| 48 | Wesentliche IT-Projekte und IT-Projektrisiken sind der Geschäftsleitung regelmäßig und anlassbezogen zu berichten. IT-Projektrisiken sind im Risikomanagement angemessen zu berücksichtigen. | |
| 49 | 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 die extern oder im Unternehmen entwickelten Anwendungen (z. B. IDV).<br><br>Die Ausgestaltung der Prozesse erfolgt entsprechend dem Risikoprofil. |
| 50 | Sowohl Anforderungen an die Funktionalität der Anwendung wie auch nichtfunktionale Anforderungen müssen sachgerecht erhoben, bewertet und dokumentiert werden. Die Verantwortung für die Erhebung und Bewertung der Anforderungen liegt in den Fachbereichen. | Anforderungsdokumente entsprechend dem gewählten Vorgehen sind beispielsweise:<br><br>■ Fachkonzept (beispielsweise User-Story),<br>■ Technisches Fachkonzept (beispielsweise Pflichtenheft oder Product Back-Log).<br><br>Nichtfunktionale Anforderungen an IT-Systeme sind beispielsweise:<br><br>■ Ergebnisse der Schutzbedarfsfeststellung,<br>■ Zugriffsregelungen,<br>■ Ergonomie,<br>■ Wartbarkeit,<br>■ Antwortzeiten,<br>■ Resilienz. |
| 51 | Im Rahmen der Anwendungsentwicklung sind nach Maßgabe des Schutzbedarfs angemessene Vorkehrungen im Hinblick darauf zu treffen, dass nach Produktivsetzung der Anwendung die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten nachvollziehbar sichergestellt werden. | Geeignete Vorkehrungen können sein:<br><br>■ Prüfung der Eingabedaten,<br>■ Systemzugangskontrolle,<br>■ Nutzer-Authentifizierung,<br>■ Transaktionsautorisierung,<br>■ Protokollierung der Systemaktivität,<br>■ Prüfpfade (Audit Logs), |

- Verfolgung von sicherheitsrelevanten Ereignissen,
- Behandlung von Ausnahmen.

52 Im Rahmen der Anwendungsentwicklung müssen 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. Die Überprüfung des Quellcodes ist eine methodische Untersuchung zur Identifizierung von Risiken.

53 Sowohl die von Dritten für das Unternehmen entwickelte als auch die im Unternehmen selbst entwickelte Anwendung ist übersichtlich und für sachkundige Dritte nachvollziehbar zu dokumentieren.

Die Dokumentation der Anwendung und ihrer Entwicklung muss zumindest folgende Fragen klären:

- Was soll entwickelt werden?
- Wie wurde die Anwendung sowohl technisch als auch prozessual entwickelt?
- Wie muss die Anwendung betrieben und eingesetzt werden?

Zur Nachvollziehbarkeit der Anwendungsentwicklung trägt beispielsweise eine Versionierung des Quellcodes und der Anforderungsdokumente bei.

54 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 Sicherheitskontrollen einzubeziehen. Sofern bei einer Anwendung die Systemleistung von Bedeutung ist, ist auch diese unter verschiedenen, sachgerechten Stressbelastungsszenarien zu testen. Die Durchführung von fachlichen Abnahmetests verantwortet der für die Anwendung zuständige Fachbereich. Testumgebungen zur Durchführung der Abnahmetests haben in für den Test wesentlichen Aspekten der Produktionsumgebung zu entsprechen. Testaktivitäten und Testergebnisse sind zu dokumentieren.

Dies umfasst eine einschlägige Expertise sowie eine angemessen ausgestaltete Unabhängigkeit von den Anwendungsentwicklern.

Eine Testdokumentation enthält mindestens folgende Punkte:

- Testfallbeschreibung,
- Dokumentation der zugrunde gelegten Parametrisierung des Testfalls,
- Testdaten,
- erwartetes Testergebnis,
- erzieltes Testergebnis,
- aus den Tests abgeleitete Maßnahmen.

55 Nach Produktivsetzung der 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.

56 Ein angemessenes Verfahren für die Klassifizierung/Kategorisierung (Schutzbedarfsklasse) und den Umgang mit den von Endbenutzern des Fachbereichs entwickelten oder betriebenen Anwendungen ist festzulegen.

Die Einhaltung von Programmierstandards wird auch für die von Endbenutzern in den Fachbereichen entwickelten Anwendungen (z. B. IDV-Anwendung) sichergestellt. Jede dieser Anwendungen wird einer Schutzbedarfsklasse zugeordnet. Übersteigt der ermittelte Schutzbedarf die technische Schutzmöglichkeit dieser Anwendungen, werden Schutzmaßnahmen in Abhängigkeit der Ergebnisse der Schutzbedarfsklassifizierung ergriffen.

57 Die Vorgaben zur Identifizierung der von Endbenutzern 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 verantwortliche(r) Mitarbeiter,
- Technologie,
- Ergebnis der Risikoklassifizierung/Schutzbedarfseinstufung und ggf. die daraus abgeleiteten Schutzmaßnahmen.

## 7. IT-Betrieb (inkl. Datensicherung)

58 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.

59 Die Komponenten der IT-Systeme sowie 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,
- 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 Zeitraum der Nichtverfügbarkeit der IT-Systeme sowie der maximal tolerierbare Datenverlust.

60 Das Portfolio aus IT-Systemen ist angemessen zu steuern. Hierbei werden auch die Risiken aus veralteten IT-Systemen berücksichtigt (Lebens-Zyklus Management).

61 Die Prozesse zur Änderung von IT-Systemen sind abhängig vom Risikoprofil auszugestalten und umzusetzen. Dies gilt ebenso für Neu- oder Ersatzbeschaffungen von IT-Systemen sowie für sicherheitsrelevante Nachbesserungen (Sicherheitspatches).

Beispiele für Änderungen sind:

- Funktionserweiterungen oder Fehlerbehebungen von Software-Komponenten,
- Datenmigrationen,
- Änderungen an Konfigurationseinstellungen von IT-Systemen,
- Austausch von Hardware-Komponenten (Server, Router etc.),
- Einsatz neuer Hardware-Komponenten,
- Umzug der IT-Systeme zu einem anderen Standort.

62 Anträge zur Änderung von IT-Systemen 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.

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).

63 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. 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 Geschäftsleitung 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.

64 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 und zur Lesbarkeit von Datensicherungen sind regelmäßig, mindestens jährlich, im Rahmen einer Stichprobe sowie anlassbezogen zu testen.

Die Anforderungen an die Ausgestaltung und Lagerung der Datensicherungen 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. Ausgliederungen von IT-Dienstleistungen und sonstige Dienstleistungsbeziehungen im Bereich IT-Dienstleistungen; isolierter Bezug von Hard- und/oder Software

65 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 Dienstleistungsunternehmen 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).

66 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 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.

67 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.

68 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, die im Regelfall den Zielvorgaben des Unternehmens entsprechen.

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 zu berücksichtigen.

69 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.

---

70 II. Rn. 66 bis 69 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.

---

# 9. Kritische Infrastrukturen

71 Dieses Modul richtet sich - im Kontext mit den anderen Modulen 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[1]).

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.

Dieses Modul 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.

72 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 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.

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

73 Im Rahmen des Informationsrisiko- und Informationssicherheits-managements gemäß den VAIT-Modulen 3 und 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.

Hierzu sind insbesondere solche Maßnahmen geeignet, mit denen den Risiken für die Verfügbarkeit bei einem hohen und sehr hohen Schutzbedarf begegnet werden kann.

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, 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.

74 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 VAIT zu berücksichtigen.
- Im Rahmen der Notfallvorsorge sind Maßnahmen zu ergreifen, mit denen die kritischen Dienstleistungen auch im Notfall aufrechterhalten werden können.

75 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.