BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021

An alle Kreditinstitute und Finanzdienstleistungsinstitute in der Bundesrepublik Deutschland

Bankaufsichtliche Anforderungen an die IT (BAIT)

Inhalt

I. Vorbemerkung

1 Der Anwenderkreis dieses Rundschreibens ergibt sich aus AT 2.1 MaRisk entsprechend.

2 Der Einsatz von Informationstechnik (IT) in den Instituten, auch unter Einbeziehung von IT-Services, die durch IT-Dienstleister bereitgestellt werden, hat eine zentrale Bedeutung für die Finanzwirtschaft und wird weiter an Bedeutung gewinnen. Dieses Rundschreiben gibt auf der Grundlage des § 25a Abs. 1 des Kreditwesengesetzes (KWG) einen flexiblen und praxisnahen Rahmen für die technisch-organisatorische Ausstattung der Institute - insbesondere für das Management der IT-Ressourcen, das Informationsrisikomanagement und das Informationssicherheitsmanagement - vor. Es präzisiert ferner die Anforderungen des § 25b KWG (Auslagerung von Aktivitäten und Prozessen).

3 Die in den Mindestanforderungen an das Risikomanagement (MaRisk) enthaltenen Anforderungen bleiben davon unberührt und werden im Rahmen seines Gegenstands durch dieses Rundschreiben konkretisiert. Die Themenbereiche dieses Rundschreibens sind nach Regelungstiefe und –umfang nicht abschließender Natur. Das Institut bleibt folglich jenseits der Konkretisierungen in diesem Rundschreiben gemäß § 25a Abs. 1 Satz 3 Nr. 4 KWG i. V. m. AT 7.2 Tz. 2 MaRisk verpflichtet, bei der Ausgestaltung der IT-Systeme und der dazugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Zu diesen zählen beispielsweise der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik und die internationalen Sicherheitsstandards ISO/IEC 270XX der International Organization for Standardization.

4 Die prinzipienorientierten Anforderungen dieses Rundschreibens ermöglichen die Umsetzung des Prinzips der doppelten Proportionalität (vgl. insbesondere AT 1 Tzn. 3, 5 und 7 sowie AT 2.1 Tz. 2 MaRisk).

II. Anforderungen

1. IT-Strategie

1.1. Die IT-Strategie hat die Anforderungen nach AT 4.2 der MaRisk zu erfüllen. Dies beinhaltet insbesondere, dass die Geschäftsleitung eine nachhaltige IT-Strategie festlegt, in der die Ziele sowie die Maßnahmen zur Erreichung dieser Ziele dargestellt werden.

1.2. Die Geschäftsleitung hat eine mit der Geschäftsstrategie konsistente IT-Strategie festzulegen. Mindestinhalte sind:

(a) Strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation des Instituts sowie IT-Dienstleistungen und sonstige wichtige Abhängigkeiten von Dritten

(b) Zuordnung der gängigen Standards, an denen sich das Institut orientiert, 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 Informationssicherheitsbelange

(f) Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen (Hardware- und Software-Komponenten).

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 Zentralbankfunktionen, Informationsdiensten, Telekommunikationsdienstleistungen, Versorgungsleistungen). Aussagen zu Auslagerungen von IT-Dienstleistungen können auch in den strategischen Ausführungen zu Auslagerungen enthalten sein.

Zu (b): Auswahl der gängigen Standards und Umsetzung auf die IT-Prozesse und das Informationssicherheitsmanagement des Instituts sowie Darstellung des avisierten Implementierungsumfangs der jeweiligen Standards.

Zu (c): Beschreibung der Bedeutung der Informationssicherheit im Institut 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.

Zu (d): Darstellung des Zielbilds der IT-Architektur in Form eines Überblicks über die Anwendungslandschaft.

2. IT-Governance

2.1.	Die IT-Governance 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 Regelungen zur IT-Aufbau- und IT-Ablauforganisation (vgl. AT 4.3.1 MaRisk), zum Informationsrisiko- sowie Informationssicherheitsmanagement (vgl. AT 4.3.2 MaRisk, AT 7.2 Tzn. 2 und 4 MaRisk), zur quantitativ und qualitativ angemessenen Personalausstattung der IT (vgl. AT 7.1 MaRisk) sowie zum Umfang und zur Qualität der technisch-organisatorischen Ausstattung (vgl. AT 7.2 Tz. 1 MaRisk). Regelungen für die IT-Aufbau- und IT-Ablauforganisation sind bei Veränderungen der Aktivitäten und Prozesse zeitnah anzupassen (vgl. AT 5 Tzn. 1 und 2 MaRisk).	
2.2.	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. Es ist sicherzustellen, dass diese Regelungen wirksam umgesetzt werden.	
2.3.	Das Institut hat insbesondere das Informationsrisikomanagement, das Informationssicherheitsmanagement, den IT-Betrieb und die Anwendungsentwicklung quantitativ und qualitativ angemessen mit Ressourcen auszustatten.	Hinsichtlich der Maßnahmen zur Erhaltung einer angemessenen qualitativen Ressourcenausstattung (personelle, finanzielle und sonstige Ressourcen) werden insbesondere der Stand der Technik sowie die aktuelle und zukünftige Bedrohungslage berücksichtigt.
2.4.	Interessenkonflikte und unvereinbare Tätigkeiten innerhalb der IT-Aufbau- und IT-Ablauforganisation sind zu vermeiden.	Interessenkonflikten zwischen Aktivitäten, die beispielsweise im Zusammenhang mit der Anwendungsentwicklung und den Aufgaben des IT-Betriebs stehen, kann durch aufbau- oder ablauforganisatorische Maßnahmen, bzw. durch eine adäquate Rollendefinition begegnet werden.

2.5.	Zur Steuerung der für den Betrieb und die Weiterentwicklung der IT-Systeme zuständigen Bereiche durch die Geschäftsleitung sind angemessene quantitative oder qualitative Kriterien durch diese festzulegen. Die Einhaltung der Kriterien ist zu überwachen.	Bei der Festlegung der Kriterien können z. B. die Qualität der Leistungserbringung, die Verfügbarkeit, Wartbarkeit, Anpassbarkeit an neue Anforderungen, Sicherheit der IT-Systeme oder der dazugehörigen IT-Prozesse sowie deren Kosten berücksichtigt werden.

3. Informationsrisikomanagement

3.1.	Die Informationsverarbeitung und -weitergabe in Geschäfts- und Serviceprozessen wird durch datenverarbeitende IT-Systeme und zugehörige IT-Prozesse unterstützt. Deren Umfang und Qualität hat sich insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie an der Risikosituation zu orientieren (vgl. AT 7.2 Tz. 1 MaRisk). IT-Systeme, die zugehörigen IT-Prozesse und sonstige Bestandteile des Informationsverbundes müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen (vgl. AT 7.2 Tz. 2 MaRisk). Das Institut hat die mit dem Management der Informationsrisiken verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege zu definieren und aufeinander abzustimmen (vgl. AT 4.3.1 Tz. 2 MaRisk). Hierfür hat das Institut angemessene Überwachungs- und Steuerungsprozesse einzurichten (vgl. AT 7.2 Tz. 4 MaRisk) und diesbezügliche Berichtspflichten zu definieren (vgl. BT 3.2 Tz. 1 MaRisk).	
3.2.	Die Bestandteile eines Systems zum Management der Informationsrisiken sind 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.
3.3.	Das Institut hat über einen aktuellen Überblick über die Bestandteile des festgelegten Informationsverbunds sowie deren Abhängigkeiten und Schnittstellen zu verfügen. Das Institut sollte sich hierbei insbesondere an den betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie an der Risikosituation orientieren.	Zu einem Informationsverbund gehören beispielsweise geschäftsrelevante Informationen, 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.

3.4.	Das Institut hat regelmäßig und anlassbezogen den Schutzbedarf für die Bestandteile seines definierten Informationsverbundes, insbesondere im Hinblick auf die Schutzziele „Integrität“, „Verfügbarkeit“, „Vertraulichkeit“ und „Authentizität“, zu ermitteln. Die Eigentümer der Information bzw. die Fachbereiche, die verantwortlich für die Geschäftsprozesse sind, verantworten die Ermittlung des Schutzbedarfes.	
3.5.	Die Schutzbedarfsfeststellung sowie die zugehörige Dokumentation sind durch das Informationsrisikomanagement zu überprüfen.	
3.6.	Das Institut hat Anforderungen zu definieren, die zur Erreichung des jeweiligen Schutzbedarfs angemessen sind, und diese in geeigneter Form zu dokumentieren (Sollmaßnahmenkatalog).	Der Sollmaßnahmenkatalog enthält lediglich die Anforderung, nicht jedoch deren konkrete Umsetzung.
3.7.	Das Institut hat auf Basis der festgelegten Risikokriterien einen Vergleich der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen (dem Ist-Zustand) durchzuführen.	Die Risikoanalyse berücksichtigt über den Soll-Ist-Vergleich hinaus u. a. mögliche Bedrohungen, das Schadenspotenzial, die Schadenshäufigkeit sowie den Risikoappetit. Sonstige risikoreduzierende Maßnahmen können hierbei berücksichtigt werden. Falls Sollmaßnahmen nicht implementiert werden können (z. B. wegen technischer Restriktionen), können sonstige risikoreduzierende Maßnahmen umgesetzt werden.
3.8.	Sonstige risikoreduzierende Maßnahmen aufgrund unvollständig umgesetzter Sollmaßnahmen sind wirksam zu koordinieren, zu dokumentieren, zu überwachen und zu steuern.	

3.9.	Das Informationsrisikomanagement hat die Risikoanalyse zu koordinieren und zu überwachen sowie deren Ergebnisse in den Prozess des Managements der operationellen Risiken zu überführen. Die Behandlung der Risiken ist kompetenzgerecht zu genehmigen.	
3.10.	Das Institut 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. Maßnahmen können z. B. die direkte Warnung von Mitarbeitern, das Sperren von betroffenen Schnittstellen und den Austausch von betroffenen IT-Systemen umfassen.
3.11.	Die Geschäftsleitung ist regelmäßig, mindestens jedoch vierteljährlich, insbesondere über die Ergebnisse der Risikoanalyse sowie Veränderungen an der Risikosituation zu unterrichten.	Die Risikosituation enthält auch externe potenzielle Bedrohungen.

4. Informationssicherheitsmanagement

4.1.	Das Informationssicherheitsmanagement macht Vorgaben zur Informationssicherheit, definiert Prozesse und steuert deren Umsetzung (vgl. AT 7.2 Tz. 2 MaRisk). Das Informationssicherheitsmanagement folgt einem fortlaufenden Prozess, der die Phasen Planung, Umsetzung, Erfolgskontrolle sowie Optimierung und Verbesserung umfasst. Die inhaltlichen Berichtspflichten des Informationssicherheitsbeauftragten an die Geschäftsleitung sowie der Turnus der Berichterstattung orientieren sich an BT 3.2 Tz. 1 MaRisk.	
4.2.	Die Geschäftsleitung hat eine Informationssicherheitsleitlinie zu beschließen und innerhalb des Instituts zu kommunizieren. Die Informationssicherheitsleitlinie hat im Einklang mit den Strategien des Instituts zu stehen. Die Leitlinie ist bei wesentlichen Veränderungen der Rahmenbedingungen zu überprüfen und bei Bedarf zeitnah anzupassen.	In der Informationssicherheitsleitlinie werden die Eckpunkte zum Schutz von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität sowie der Geltungsbereich für die Informationssicherheit festgelegt. Darüber hinaus werden die wesentlichen organisatorischen Aspekte, wie die wichtigsten Rollen

		und Verantwortlichkeiten des Informationssicherheitsmanagements beschrieben. Mit der Leitlinie legt die Geschäftsleitung u. a. dar: ■ ihre Gesamtverantwortung für die Informationssicherheit ■ Frequenz und Umfang des Berichtswesens zur Informationssicherheit ■ die Kompetenzen im Umgang mit Informationsrisiken ■ die grundlegenden Anforderungen der Informationssicherheit an Personal, Auftragnehmer, Prozesse und Technologien. Rahmenbedingungen umfassen u. a. interne Veränderungen der Aufbau- und Ablauforganisation oder der IT-Systeme sowie äußere Veränderungen z. B. der Bedrohungsszenarien, Technologien oder der rechtlichen Anforderungen.
4.3.	Auf Basis der Informationssicherheitsleitlinie und der Ergebnisse des Informationsrisikomanagements sind konkretisierende, den Stand der Technik berücksichtigende Informationssicherheitsrichtlinien und Informationssicherheitsprozesse zu definieren.	Informationssicherheitsrichtlinien werden z. B. für die Bereiche Netzwerksicherheit, Kryptografie, Identitäts- und Rechtemanagement, Protokollierung sowie physische Sicherheit (z. B. Perimeter- und Gebäudeschutz) erstellt. Informationssicherheitsprozesse dienen in erster Linie zur Erreichung der vereinbarten Schutzziele. Dazu gehört u. a., Informationssicherheitsvorfällen vorzubeugen bzw. diese zu identifizieren sowie die angemessene Reaktion und Kommunikation im weiteren Verlauf.
4.4.	Die Geschäftsleitung hat die Funktion des Informationssicherheitsbeauftragten einzurichten. Diese Funktion umfasst die Verantwortung für die Wahrnehmung aller Belange der Informationssicherheit innerhalb des Instituts und gegenüber Dritten. Sie stellt sicher, dass die in der IT-Strategie, der Informationssicherheitsleitlinie und den Informa-	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

tionssicherheitsrichtlinien des Instituts festgelegten Ziele und Maßnahmen hinsichtlich der Informationssicherheit sowohl intern als auch gegenüber Dritten transparent gemacht und deren Einhaltung regelmäßig sowie anlassbezogen überprüft und überwacht werden.

von Zielkonflikten (z. B. Wirtschaftlichkeit kontra Informationssicherheit)

- Erstellung von Informationssicherheitsrichtlinien und ggf. weiteren einschlägigen Regelungen sowie die Kontrolle ihrer Einhaltung
- den Informationssicherheitsprozess im Institut 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 Informationssicherheitsbelange
- die Realisierung von Informationssicherheitsmaßnahmen zu initiieren und zu überwachen
- Überwachung und Hinwirkung auf Einhaltung der Informationssicherheit bei Projekten und Beschaffungen
- als Ansprechpartner für Fragen der Informationssicherheit innerhalb des Instituts und für Dritte bereitzustehen
- Informationssicherheitsvorfälle zu untersuchen und an die Geschäftsleitung zu berichten
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und zu koordinieren.

Der Informationssicherheitsbeauftragte kann durch ein Informationssicherheitsmanagement-Team unterstützt werden.

4.5.	Die Funktion des Informationssicherheitsbeauftragten ist organisatorisch und prozessual unabhängig auszugestalten, um mögliche Interessenskonflikte zu vermeiden.	Zur Vermeidung möglicher Interessenkonflikte werden insbesondere folgende Maßnahmen beachtet: ■ Funktions- und Stellenbeschreibung für den Informationssicherheitsbeauftragten, seinen Vertreter und ggf. weiterer Stellen ■ Festlegung der erforderlichen Ressourcenausstattung für die Funktion des Informationssicherheitsbeauftragten ■ ein der Funktion zugewiesenes Budget für Informationssicherheitsschulungen im Institut und die persönliche Weiterbildung des Informationssicherheitsbeauftragten sowie seines Vertreters ■ unmittelbare und jederzeitige Gelegenheit zur Berichterstattung des Informationssicherheitsbeauftragten an die Geschäftsleitung ■ Verpflichtung der Beschäftigten des Instituts sowie der IT-Dienstleister zur sofortigen und umfassenden Unterrichtung des Informationssicherheitsbeauftragten über alle bekannt gewordenen informationssicherheitsrelevanten Sachverhalte, die das Institut betreffen ■ die Funktion des Informationssicherheitsbeauftragten wird von den Bereichen getrennt, die für den Betrieb und die Weiterentwicklung der IT-Systeme zuständig sind ■ der Informationssicherheitsbeauftragte nimmt keinesfalls Aufgaben der Internen Revision wahr.
4.6.	Jedes Institut hat die Funktion des Informationssicherheitsbeauftragten grundsätzlich im eigenen Haus vorzuhalten.	Im Hinblick auf regional tätige (insbesondere verbundangehörige) Institute sowie kleine (insbesondere gruppenangehörige) Institute ohne wesentliche eigenbetriebene IT mit einem gleichgerichteten Geschäftsmodell und gemeinsamen IT-Dienstleistern für die Abwicklung von bankfachlichen Prozes-

		sen ist es im Hinblick auf die regelmäßig (verbund- oder gruppenseitig) vorhandenen Kontrollmechanismen zulässig, dass mehrere Institute einen gemeinsamen Informationssicherheitsbeauftragten bestellen, wobei vertraglich sicherzustellen ist, dass dieser gemeinsame Informationssicherheitsbeauftragte die Wahrnehmung der einschlägigen Aufgaben der Funktion in allen betreffenden Instituten jederzeit gewährleisten kann. In diesem Fall ist jedoch in jedem Institut eine zuständige Ansprechperson für den Informationssicherheitsbeauftragten zu benennen. Institute können die Funktion des Informationssicherheitsbeauftragten grundsätzlich mit anderen Funktionen im Institut kombinieren. Die Möglichkeit, sich externer Unterstützung per Servicevertrag zu bedienen, bleibt für die Institute unberührt.
4.7.	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 orientiert sich am Schutzbedarf der betroffenen Bestandteile des Informationsverbundes. Ein Informationssicherheitsvorfall kann auch dann vorliegen, wenn mindestens eines der Schutzziele („Verfügbarkeit", „Integrität", „Vertraulichkeit", „Authentizität") gemäß den Vorgaben des institutsspezifischen Sollkonzepts der Informationssicherheit verletzt ist. Die Begriffe „Informationssicherheitsvorfall", „sicherheitsrelevantes Ereignis" (im Sinne der operativen Informationssicherheit) und „ungeplante Abweichung vom Regelbetrieb" (im Sinne von „Störung") werden nachvollziehbar voneinander abgegrenzt.
4.8.	Das Institut hat eine Richtlinie über das Testen und Überprüfen der Maßnahmen zum Schutz der Informationssicherheit einzuführen und	Die Richtlinie berücksichtigt u. a.: ■ die allgemeine Bedrohungslage

	diese regelmäßig und anlassbezogen zu überprüfen und bei Bedarf anzupassen.	■ die individuelle Risikosituation des Instituts ■ Kategorien von Test- und Überprüfungsobjekten (z. B. das Institut, IT-Systeme, Komponenten) ■ Art, Umfang und Frequenz von Tests und Überprüfungen ■ Zuständigkeiten und Regelungen zur Vermeidung von Interessenkonflikten.
4.9.	Das Institut hat ein kontinuierliches und angemessenes Sensibilisierungs- und Schulungsprogramm für Informationssicherheit festzulegen. Der Erfolg der festgelegten Sensibilisierungs- und Schulungsmaßnahmen ist zu überprüfen.	Das Programm sollte zielgruppenorientiert mindestens folgende Aspekte berücksichtigen: ■ persönliche Verantwortung für eigene Handlungen und Unterlassungen sowie allgemeine Verantwortlichkeiten zum Schutz von Informationen ■ grundsätzliche Verfahren zur Informationssicherheit (wie Berichterstattung über Informationssicherheitsvorfälle) und allgemeingültige Sicherheitsmaßnahmen (z. B. zu Passwörtern, Social Engineering, Prävention vor Schadsoftware und dem Verhalten bei Verdacht auf Schadsoftware).
4.10.	Der Informationssicherheitsbeauftragte hat der Geschäftsleitung regelmäßig, mindestens vierteljährlich, über den Status der Informationssicherheit sowie anlassbezogen zu berichten.	Der Statusbericht enthält beispielsweise die Bewertung der Informationssicherheitslage im Vergleich zum Vorbericht, Informationen zu Projekten zur Informationssicherheit, Informationssicherheitsvorfälle sowie Penetrationstestergebnisse.

5. 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 (vgl. AT 7.2 Tz. 2 MaRisk). 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 (vgl. AT 7.2 Tz. 4 MaRisk).

5.2. Das Institut 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 oder 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.	Es 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.
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. Die zeitnahe Analyse und Reaktion kann eine ständig besetzte zentrale Stelle, z. B. in Form eines Security Operation Centers (SOC), erfordern.
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.	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 (Gapanalysen)

		■ Schwachstellenscans ■ Penetrationstests ■ Simulationen von Angriffen.

6. Identitäts- und Rechtemanagement

6.1.	Ein Identitäts- und Rechtemanagement stellt sicher, dass den Benutzern eingeräumte Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben des Instituts entspricht. Das Identitäts- und Rechtemanagement hat die Anforderungen nach AT 4.3.1 Tz. 2, AT 7.2 Tz. 2, sowie BTO Tz. 9 der MaRisk zu erfüllen. Jegliche Zugriffs-, Zugangs- und Zutrittsrechte auf Bestandteile bzw. zu Bestandteilen des Informationsverbundes sollten standardisierten Prozessen und Kontrollen unterliegen.	
6.2.	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 bereitgestellten Berechtigungen fest. Berechtigungskonzepte haben die Vergabe von Berechtigungen nach dem Sparsamkeitsgrundsatz („Need-to-know" und „Least-Privilege" Prinzipien) sicherzustellen, die Funktionstrennung auch berechtigungskonzeptübergreifend zu wahren und Interessenskonflikte zu vermeiden. Berechtigungskonzepte sind regelmäßig und anlassbezogen zu überprüfen und ggf. zu aktualisieren.	Eine mögliche Nutzungsbedingung ist die Befristung von eingeräumten Berechtigungen. Berechtigungen können, je nach Art, für personalisierte sowie für nicht personalisierte Benutzer (inkl. technische Benutzer) vorliegen. Zugangs- und Zugriffsberechtigungen auf den IT-Systemen können auf allen Ebenen eines IT-Systems (z. B. Betriebssystem, Datenbank, Anwendung) 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.
6.3.	Zugriffe und Zugänge müssen jederzeit zweifelsfrei einer handelnden bzw. verantwortlichen Person (möglichst automatisiert) zuzuordnen sein.	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.

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 angemessen einzubinden, so dass sie ihrer fachlichen Verantwortung nachkommen kann.	Die Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen umfassen jeweils auch die zeitnahe oder unverzügliche Umsetzung 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).
6.5.	Bei der Überprüfung, ob die eingeräumten Berechtigungen weiterhin benötigt werden und ob diese den Vorgaben des Berechtigungskonzepts entsprechen (Rezertifizierung), sind die für die Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen zuständigen Kontrollinstanzen einzubeziehen.	Fällt im Rahmen der Rezertifizierung auf, dass nicht legitimierte Berechtigungen vorhanden sind, so werden diese gemäß Regelverfahren zeitnah entzogen und bei Bedarf weitere Maßnahmen (z. B. Ursachenanalyse, Vorfallmeldung) ergriffen.
6.6.	Die Einrichtung, Änderung, Deaktivierung sowie Löschung von Berechtigungen und die Rezertifizierung sind nachvollziehbar und auswertbar zu dokumentieren.	
6.7.	Das Institut hat nach Maßgabe des Schutzbedarfs und der Soll-Anforderungen Prozesse zur Protokollierung und Überwachung einzurichten, die überprüfbar machen, dass die Berechtigungen nur wie vorgesehen eingesetzt werden. Aufgrund der damit verbundenen weitreichenden Eingriffsmöglichkeiten hat das Institut insbesondere für die Aktivitäten mit privilegierten (besonders kritischen) Benutzer- und Zutrittsrechten angemessene Prozesse zur Protokollierung und Überwachung einzurichten.	Die übergeordnete Verantwortung für die Prozesse zur Protokollierung und Überwachung von Berechtigungen wird einer Stelle zugeordnet, die unabhängig vom berechtigten Benutzer oder dessen Organisationseinheit ist. Zu privilegierten Zutrittsrechten zählen in der Regel die Rechte zum Zutritt zu Rechenzentren, Technikräumen sowie sonstigen sensiblen Bereichen.

6.8.	Durch begleitende technisch-organisatorische Maßnahmen ist einer Umgehung der Vorgaben der Berechtigungskonzepte vorzubeugen.	Technisch-organisatorische Maßnahmen sind beispielsweise: ■ Auswahl angemessener Authentifizierungsverfahren (u. a. starke Authentifizierung im Falle von Fernzugriffen) ■ Implementierung einer Richtlinie zur Wahl sicherer Passwörter ■ automatische passwortgesicherte Bildschirmsperre ■ Verschlüsselung von Daten ■ manipulationssichere Implementierung der Protokollierung ■ Maßnahmen zur Sensibilisierung der Mitarbeiter.

7. IT-Projekte und Anwendungsentwicklung

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 im Rahmen einer Auswirkungsanalyse zu bewerten (vgl. AT 8.2 Tz. 1 MaRisk). Im Hinblick auf den erstmaligen Einsatz sowie wesentliche Veränderungen von IT-Systemen sind die Anforderungen des AT 7.2 (insbesondere Tz. 3 und Tz. 5) MaRisk, AT 8.2 Tz. 1 MaRisk sowie AT 8.3 Tz. 1 MaRisk zu erfüllen.	
7.2.	Die organisatorischen Grundlagen für IT-Projekte und die Kriterien für deren Anwendung sind zu regeln.	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).
7.3.	IT-Projekte sind angemessen unter Berücksichtigung ihrer Ziele und Risiken im Hinblick auf die Dauer, Ressourcen und Qualität zu steuern. 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.
7.4.	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.
7.5.	Über wesentliche IT-Projekte und IT-Projektrisiken wird der Geschäftsleitung regelmäßig und anlassbezogen berichtet. Wesentliche Projektrisiken sind im Risikomanagement zu berücksichtigen.	
7.6.	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 u. a. die Erstellung von Software für Geschäfts- und Unterstützungsprozesse (einschließlich individueller Datenverarbeitung – IDV). Die Ausgestaltung der Prozesse erfolgt risikoorientiert.
7.7.	Anforderungen an die Funktionalität der Anwendung müssen ebenso erhoben, bewertet, dokumentiert und genehmigt werden wie nichtfunktionale Anforderungen. Zu jeder Anforderung sind entsprechende Akzeptanz- und Testkriterien zu definieren. Die Verantwortung für die Erhebung, Bewertung und Genehmigung der fachlichen	Anforderungsdokumente können sich nach Vorgehensmodell unterscheiden und beinhalten beispielsweise: ■ Fachkonzept (Lastenheft) ■ Technisches Fachkonzept (Pflichtenheft)

	Anforderungen (funktional und nicht funktional) haben die fachlich verantwortlichen Stellen zu tragen.	■ User-Story/Product Back-Log. Nichtfunktionale Anforderungen an IT-Systeme sind beispielsweise: ■ Anforderungen an die Informationssicherheit ■ Zugriffsregelungen ■ Ergonomie ■ Wartbarkeit ■ Antwortzeiten ■ Resilienz.
7.8.	Im Rahmen der Anwendungsentwicklung sind je nach Schutzbedarf angemessene Vorkehrungen zu treffen, dass auch nach jeder Produktivsetzung einer Anwendung die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten nachvollziehbar sichergestellt werden.	Geeignete Vorkehrungen sind z. B.: ■ Prüfung der Eingabedaten ■ Systemzugangskontrolle ■ Benutzerauthentifizierung ■ Transaktionsautorisierung ■ Protokollierung der Systemaktivität ■ Prüfpfade (Audit Logs) ■ Verfolgung von sicherheitsrelevanten Ereignissen ■ Behandlung von Ausnahmen.

7.9.	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 sein. Die Überprüfung des Quellcodes ist eine methodische Untersuchung zur Identifizierung von Risiken.
7.10.	Die Anwendung sowie deren Entwicklung sind übersichtlich und für sachkundige Dritte nachvollziehbar zu dokumentieren.	Die Dokumentation der Anwendung umfasst mindestens folgende Inhalte: ■ Anwenderdokumentation ■ Technische Systemdokumentation ■ Betriebsdokumentation. Zur Nachvollziehbarkeit der Anwendungsentwicklung trägt beispielsweise eine Versionierung des Quellcodes und der Anforderungsdokumente bei.
7.11.	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, die implementierten Maßnahmen zum Schutz der Informationen und bei Relevanz die Systemleistung unter verschiedenen Stressbelastungsszenarien einzubeziehen. Die fachlich zuständigen Stellen haben die Durchführung von Abnahmetests zu verantworten. Testumgebungen zur Durchführung der Abnahmetests haben in für den Test wesentlichen Aspekten der Produktionsumgebung zu entsprechen. Testaktivitäten und Testergebnisse sind zu dokumentieren.	Die Testdurchführung erfordert einschlägige Expertise der Tester 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 abgeleiteten Maßnahmen.

		Risikoorientiert schließen die Maßnahmen zum Schutz der Informationen auch Penetrationstests ein.
7.12.	Nach Produktivsetzung der Anwendung sind mögliche Abweichungen vom Regelbetrieb zu überwachen, deren Ursachen zu untersuchen und ggf. Maßnahmen zur Nachbesserung zu veranlassen.	Hinweise auf erhebliche Mängel können z. B. Häufungen von Abweichungen vom Regelbetrieb sein.
7.13.	Ein angemessenes Verfahren für die Klassifizierung/Kategorisierung (Schutzbedarfsklasse) und den Umgang mit den von Mitarbeitern des Fachbereichs entwickelten oder betriebenen Anwendungen ist festzulegen (Individuelle Datenverarbeitung – IDV).	Die Einhaltung von Programmierrichtlinien wird auch für die entwickelten IDV-Anwendungen sichergestellt. Jede Anwendung wird einer Schutzbedarfsklasse zugeordnet. Übersteigt der ermittelte Schutzbedarf die technische Schutzmöglichkeit einer Anwendungen, werden Schutzmaßnahmen in Abhängigkeit der Ergebnisse der Schutzbedarfsklassifizierung ergriffen.
7.14.	Die Vorgaben zur Identifizierung aller von Mitarbeitern des Fachbereichs entwickelten oder betriebenen Anwendungen, zur Dokumentation, zu den Programmierrichtlinien und zur Methodik des Testens, 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 für Anwendungen geführt und 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.

8. IT-Betrieb

8.1. Der IT-Betrieb hat die Anforderungen, die sich aus der Umsetzung der Geschäftsstrategie sowie aus den IT-unterstützten Geschäftsprozessen ergeben, zu erfüllen (vgl. AT 7.2 Tz. 1 und Tz. 2 MaRisk).

8.2. Die Komponenten der IT-Systeme und deren Beziehungen zueinander sind in geeigneter Weise zu verwalten, und die hierzu erfassten Bestandsangaben 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
- Schutzbedarf der IT-Systeme und deren Komponenten
- Akzeptierter Zeitraum der Nichtverfügbarkeit der IT-Systeme sowie der maximal tolerierbare Datenverlust.

8.3. Das Portfolio aus IT-Systemen bedarf der Steuerung. IT-Systeme sollten regelmäßig aktualisiert werden. Risiken aus veralteten bzw. nicht mehr vom Hersteller unterstützten IT-Systemen sind zu steuern (Lebenszyklus-Management).

8.4.	Die Prozesse zur Änderung von IT-Systemen sind abhängig von Art, Umfang, Komplexität und Risikogehalt auszugestalten und umzusetzen. Dies gilt auch für Neu- bzw. 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 Softwarekomponenten ■ Datenmigrationen ■ Änderungen an Konfigurationseinstellungen von IT-Systemen ■ Austausch von Hardwarekomponenten (Server, Router etc.) ■ Einsatz neuer Hardwarekomponenten ■ Umzug der IT-Systeme zu einem anderen Standort.
8.5.	Änderungen von IT-Systemen sind in geordneter Art und Weise aufzunehmen, zu dokumentieren, unter Berücksichtigung möglicher Umsetzungsrisiken zu bewerten, zu priorisieren, zu genehmigen sowie 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 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).
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, wie auch die Angemessenheit der Bewertung und Priorisierung, ist zu überwachen und zu steuern. Das Institut 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. Hier können standardisierte Incident– und Problemmanagement-Lösungen eingesetzt werden.

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 Wiederherstellung und zur Gewährleistung der Lesbarkeit der Daten sind regelmäßig, mindestens jährlich, im Rahmen einer Stichprobe sowie anlassbezogen zu testen.	Die Anforderungen an die Maßnahmen zur Sicherstellung von Verfügbarkeit, Lesbarkeit und Aktualität der 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.	

9. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

9.1.	IT-Dienstleistungen umfassen alle Ausprägungen des Bezugs von IT; dazu zählen insbesondere die Bereitstellung von IT-Systemen, Projekte/Gewerke oder Personalgestellung. Die Auslagerungen der IT-Dienstleistungen haben die Anforderungen nach AT 9 der MaRisk zu erfüllen. Dies gilt auch für Auslagerungen von IT-Dienstleistungen, die dem Institut 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). Das Institut hat auch beim sonstigen Fremdbezug von IT-Dienstleistungen die allgemeinen Anforderungen an die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 25a Abs. 1 KWG zu beachten	

	(vgl. AT 9 Tz. 1 – Erläuterungen - MaRisk). Bei jedem Bezug von Software sind die damit verbundenen Risiken angemessen zu bewerten (vgl. AT 7.2 Tz. 4 Satz 2 MaRisk).	
9.2.	Wegen der grundlegenden Bedeutung der IT für das Institut ist auch für jeden sonstigen Fremdbezug von IT-Dienstleistungen vorab eine Risikobewertung durchzuführen.	Art und Umfang einer Risikobewertung kann das Institut unter Proportionalitätsgesichtspunkten nach Maßgabe seines allgemeinen Risikomanagements flexibel festlegen. Für gleichartige Formen des sonstigen Fremdbezugs von IT-Dienstleistungen kann auf bestehende Risikobewertungen zurückgegriffen werden. Die für Informationssicherheit und Notfallmanagement verantwortlichen Funktionen des Instituts werden eingebunden.
9.3.	Der sonstige Fremdbezug von IT-Dienstleistungen ist im Einklang mit den Strategien unter Berücksichtigung der Risikobewertung des Instituts zu steuern. Die Erbringung der vom Dienstleister geschuldeten Leistung ist entsprechend der Risikobewertung zu überwachen.	Hierfür wird eine vollständige, strukturierte Vertragsübersicht vorgehalten. Die Steuerung kann auf der Basis dieser Vertragsübersicht durch Bündelung von Verträgen des sonstigen Fremdbezugs von IT-Dienstleistungen (Vertragsportfolio) erfolgen. Bestehende Steuerungsmechanismen können hierzu genutzt werden.
9.4.	Die aus der Risikobewertung zum sonstigen Fremdbezug von IT-Dienstleistungen abgeleiteten Maßnahmen sind angemessen in der Vertragsgestaltung zu berücksichtigen. Die Ergebnisse der Risikobewertung 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, zum Notfallmanagement und zum IT-Betrieb, die im Regelfall den Zielvorgaben des Instituts entsprechen. Bei Relevanz wird auch die Möglichkeit eines Ausfalls eines IT-Dienstleisters berücksichtigt und eine diesbezügliche Exit- bzw. Alternativ-Strategie entwickelt und dokumentiert. Als erforderlich erkannte Maßnahmen sind auch im Fall der Einbindung von Subunternehmen des IT-Dienstleisters zu berücksichtigen.

9.5.	Die Risikobewertungen in Bezug auf den sonstigen Fremdbezug von IT-Dienstleistungen sind regelmäßig und anlassbezogen zu überprüfen und ggf. inkl. der Vertragsinhalte anzupassen.	

10. IT-Notfallmanagement

10.1.	Das Institut hat Ziele zum Notfallmanagement zu definieren und hieraus abgeleitet einen Notfallmanagementprozess festzulegen. Für Notfälle in zeitkritischen Aktivitäten und Prozessen ist Vorsorge zu treffen (Notfallkonzept). Die im Notfallkonzept festgelegten Maßnahmen müssen dazu geeignet sein, das Ausmaß möglicher Schäden zu reduzieren (vgl. AT 7.3 Tz. 1 MaRisk). Das Notfallkonzept muss Geschäftsfortführungs- sowie Wiederherstellungspläne umfassen. Im Fall der Auslagerung von zeitkritischen Aktivitäten und Prozessen haben das auslagernde Institut und das Auslagerungsunternehmen über aufeinander abgestimmte Notfallkonzepte zu verfügen (vgl. AT 7.3 Tz. 2 MaRisk). Die Wirksamkeit und Angemessenheit des Notfallkonzeptes ist regelmäßig zu überprüfen. Für zeitkritische Aktivitäten und Prozesse ist sie für alle relevanten Szenarien mindestens jährlich und anlassbezogen nachzuweisen (vgl. AT 7.3 Tz. 3 MaRisk).	
10.2.	Die Ziele und Rahmenbedingungen des IT-Notfallmanagements sind auf Basis der Ziele des Notfallmanagements festzulegen.	Rahmenbedingungen enthalten u. a. organisatorische Aspekte wie z. B. Schnittstellen zu anderen Bereichen (u. a. Risikomanagement oder Informationssicherheitsmanagement).
10.3.	Das Institut hat auf Basis des Notfallkonzepts für IT-Systeme, welche zeitkritische Aktivitäten und Prozesse unterstützen, IT-Notfallpläne zu erstellen.	IT-Notfallpläne umfassen Wiederanlauf-, Notbetriebs- und Wiederherstellungspläne sowie die dafür festgelegten Parameter und berücksichtigen Abhängigkeiten, um die zeitkritischen Aktivitäten und Prozesse wiederherzustellen. 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 Instituts und der (IT-) Dienstleister ■ Abhängigkeiten bei der Wiederherstellungspriorisierung der IT-Prozesse und -Systeme ■ Notwendige Ressourcen, um eine (eingeschränkte) Fortführung der Geschäftsprozesse zu gewährleisten ■ Abhängigkeiten von externen Faktoren (Gesetzgeber, Anteilseigner, Öffentlichkeit, etc.).
10.4.	Die Wirksamkeit der IT-Notfallpläne ist durch mindestens jährliche IT-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 IT-Testkonzept zu erstellen.	Das IT-Testkonzept beinhaltet sowohl Tests einzelner IT-Systeme (z. B. Komponenten, einzelne Anwendungen) als auch deren Zusammenfassung zu Systemverbünden (z. B. Hochverfügbarkeitscluster) sowie Prozesse (z. B. Zutritts- und Zugriffsmanagement).
10.5.	Das Institut 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 IT-Normalbetriebs erbracht werden können.	

11. Management der Beziehungen mit Zahlungsdienstnutzern

11.1.	Die nach § 53 ZAG geforderten Risikominderungsmaßnahmen zur Beherrschung der operationellen und sicherheitsrelevanten Risiken beinhalten auch Maßnahmen, mit denen die Zahlungsdienstnutzer für die Reduzierung, insbesondere von Betrugsrisiken, direkt adressiert werden. Dazu ist ein angemessenes Management der Beziehungen mit den Zahlungsdienstnutzern zu etablieren.	
11.2.	Das Institut hat Prozesse einzurichten und zu implementieren, durch die das Bewusstsein der Zahlungsdienstnutzer über die sicherheitsrelevanten Risiken in Bezug auf die Zahlungsdienste verbessert wird, indem die Zahlungsdienstnutzer unterstützt und beraten werden.	Betroffen sind insbesondere Kommunikationsprozesse zur Sensibilisierung der eigenen Zahlungsdienstnutzer für Risiken bei der Nutzung von Zahlungsdiensten. Die Sensibilisierung kann in Form allgemeiner Ansprachen (Informationen auf der Web-Seite) oder bei Bedarf durch individuelle Ansprachen erfolgen. Die Prozesse werden an die spezifische aktuelle Risiko- und Bedrohungslage angepasst und können sich in Bezug auf einzelne Zahlungsdienstnutzer unterscheiden.
11.3.	Die den Zahlungsdienstnutzern angebotene Unterstützung und Beratung sind aktuell zu halten und an neue Risikolagen anzupassen. Anpassungen sind dem Zahlungsdienstnutzer in angemessener Form zu kommunizieren.	Im Ergebnis sollte es dem Zahlungsdienstnutzer ermöglicht werden, auf aktuelle Risiken angemessen zu reagieren und den Zahlungsdienst sicher nutzen zu können.
11.4.	Das Institut hat – wenn die Produktfunktionalität es zulässt – dem Zahlungsdienstnutzer die Möglichkeit zu bieten, einzelne der angebotenen Zahlungsfunktionalitäten zu deaktivieren.	Eine solche Deaktivierung kann z. B. eine Sperrmöglichkeit für Auslandsüberweisungen außerhalb des SEPA-Raums beinhalten. Entsprechende Anträge können online oder auch auf schriftlichem Wege übermittelt werden.
11.5.	Falls das Institut mit dem Zahlungsdienstnutzer Betragsobergrenzen vereinbart hat, ist dem Zahlungsdienstnutzer die Möglichkeit zu geben, die vereinbarten Grenzen anzupassen.	Dies kann z. B. eine Anpassung des Tageslimits für Überweisungen im Online-Banking beinhalten.

11.6.	Zur Erkennung von betrügerischer oder nicht autorisierter Nutzung der Zahlungskonten des Zahlungsdienstnutzers hat das Institut dem Zahlungsdienstnutzer die Möglichkeit einzuräumen, Benachrichtigungen über getätigte und fehlgeschlagene Transaktionen zu erhalten.	Ziel ist es, dem Zahlungsdienstnutzer eine angemessene eigene Kontrolle der durchgeführten Transaktionen oder Transaktionsversuche zu ermöglichen, so dass betrügerische Transaktionen oder Betrugsversuche von diesem möglichst früh auch selbst erkannt werden können. Eine ständige und sofortige explizite Benachrichtigung über alle Transaktionen und Transaktionsversuche ist nicht erforderlich. Vom Institut durchzuführende Betrugserkennungsmaßnahmen bleiben davon unberührt.
11.7.	Das Institut hat die Zahlungsdienstnutzer zeitnah über Aktualisierungen der Sicherheitsverfahren zu informieren, die in Bezug auf die Erbringung von Zahlungsdiensten Auswirkungen auf die Zahlungsdienstnutzer haben.	Der konkrete Kommunikationsweg wird vom Institut bestimmt. Dem Zahlungsdienstnutzer sollte die Möglichkeit gegeben werden, sich auf geänderte Prozesse angemessen einzustellen und sich vorzubereiten, um die Zahlungsdienste möglichst ohne Unterbrechungen nutzen zu können.
11.8.	Das Institut hat die Zahlungsdienstnutzer in Bezug auf alle Fragen, Unterstützungsanfragen, Benachrichtigungen über Unregelmäßigkeiten oder alle sicherheitsrelevanten Fragen hinsichtlich der Zahlungsdienste zu unterstützen. Die Zahlungsdienstnutzer sind angemessen darüber zu informieren, wie sie diese Unterstützung erhalten können.	Es werden angemessene und für alle Zahlungsdienstnutzer zu nutzende Kommunikationskanäle eingerichtet. Diese können z. B. über die Web-Seiten, über technische Kommunikationskanäle oder in schriftlicher Kommunikation bekannt gemacht werden.

12. Kritische Infrastrukturen

12.1.	Dieses Kapitel richtet sich – im Kontext mit den anderen Kapiteln der BAIT und den sonstigen einschlägigen bankaufsichtlichen 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]).

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

Es ergänzt insoweit die bankaufsichtlichen Anforderungen an die IT um Anforderungen an die wirksame Umsetzung besonderer Maßnahmen zum Erreichen des KRITIS-Schutzziels. Als KRITIS-Schutzziel wird nachfolgend das Bewahren der Versorgungssicherheit der Gesellschaft mit den in § 7 BSI-Kritisverordnung genannten kritischen Dienstleistungen (Bargeldversorgung, kartengestützter Zahlungsverkehr, konventioneller Zahlungsverkehr sowie Verrechnung und Abwicklung von Wertpapier- und Derivatgeschäften) 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 Auslagerungen 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 und Konzepte der Hochverfügbarkeit berücksichtigen. Dabei soll der Stand der Technik eingehalten werden.

Dieses Kapitel kann optional verwendet werden, um im Rahmen einer Jahresabschlussprüfung den Nachweis nach § 8a Abs. 3 BSIG zu erbringen. Dazu müssen alle informationstechnischen Systeme, Komponenten oder Prozesse der kritischen Infrastrukturen in der Prüfung komplett abgedeckt sein.

Alternativ können die KRITIS-Betreiber einen unternehmensindividuellen Ansatz verfolgen oder einen branchenspezifischen Sicherheitsstandard (B3S) gemäß § 8a Abs. 2 BSIG erstellen. Der Nachweis gemäß § 8a Abs. 3 BSIG ist in diesen Fällen unter Hinzuziehung einer geeigneten prüfenden Stelle (siehe einschlägige FAQ auf der BSI-Website) zu erstellen.

12.2.	Der Geltungsbereich der kritischen Infrastrukturen innerhalb des Informationsverbundes ist eindeutig zu kennzeichnen. Hierbei sind alle relevanten Schnittstellen einzubeziehen. Alle einschlägigen Anforderungen der BAIT 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 im Inventar entsprechend 3.3. BAIT (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.

12.3.	Im Rahmen des Informationsrisiko- und Informationssicherheitsmanagements gemäß den BAIT-Kapiteln 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. Unter anderem sollten daher Konzepte der Hochverfügbarkeit geprüft und soweit geeignet, angewandt werden.	Grundsätzlich sind für Risiken Maßnahmen zur Mitigation zu treffen. Dabei soll der Stand der Technik eingehalten werden. 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.
12.4.	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 Auslagerungen von Dienstleistungen entsprechend §§ 25a, 25b KWG i. V. m. AT 9 und AT 5 Tz. 3. f) MaRisk sowie Kapitel 9. BAIT zu berücksichtigen ■ im Rahmen der Notfallvorsorge sind Maßnahmen zu ergreifen (AT 7.3 MaRisk sowie Kapitel 10. BAIT), mit denen die kritischen Dienstleistungen auch im Notfall aufrechterhalten werden können.
12.5.	Die Nachweiserbringung gemäß § 8a Abs. 3 BSIG bzgl. der Einhaltung der Anforderungen gemäß § 8a Abs. 1 BSIG kann im Rahmen der Jahresabschlussprüfung erfolgen. Der KRITIS-Betreiber hat die einschlägigen Nachweisdokumente fristgerecht beim BSI einzureichen, entsprechend den jeweils gültigen Vorgaben des BSI.	Bei der Nachweiserbringung im Rahmen der Jahresabschlussprüfung sollte die Einhaltung der Anforderungen gemäß § 8a Abs. 1 BSIG durch den KRITIS-Betreiber erstmals auf den Jahresabschluss 2018 referenziert werden und ist anschließend mindestens alle zwei Jahre gegenüber dem BSI nachzuweisen.

	Neben der Prüfung im Rahmen des Jahresabschlusses 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.