Rundschreiben 11/2021 (BA) in der Fassung vom 16.08.2021

An alle Zahlungsinstitute und E-Geld-Institute in der Bundesrepublik Deutschland

Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (ZAIT)

Inhalt

I. Vorbemerkung

1 Die Anforderungen dieses Rundschreibens gelten für alle Institute im Sinne von § 1 Abs. 3 des Zahlungsdiensteaufsichtsgesetzes (ZAG), das heißt für Zahlungsinstitute und E-Geld-Institute (im Folgenden Institute genannt). Sie gelten auch für die Zweigniederlassungen deutscher Institute im Ausland im Sinne von § 38 ZAG. Auf Zweigniederlassungen von Unternehmen mit Sitz in einem anderen Staat des Europäischen Wirtschaftsraums nach § 39 ZAG finden sie keine Anwendung.

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 § 27 Abs. 1 ZAG 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 § 26 ZAG (Auslagerung von Aktivitäten und Prozessen) sowie die Anforderungen des § 53 Abs. 1 ZAG (Beherrschung operationeller und sicherheitsrelevanter Risiken bei der Erbringung von Zahlungsdiensten).

3 Die Themenbereiche dieses Rundschreibens sind nach Regelungstiefe und -umfang nicht abschließender Natur. Das Institut bleibt folglich jenseits der Konkretisierungen in diesem Rundschreiben verpflichtet, bei der Ausgestaltung der IT-Systeme und der dazugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Zu diesen zählen bspw. der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik, die internationalen Sicherheitsstandards ISO/IEC 270XX der International Organization for Standardization und der Payment Card Industry Data Security Standard (PCI-DSS).

4 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 dieses Rundschreibens sind durch angemessene Maßnahmen der Unternehmenssteuerung, Kontrollmechanismen und Verfahren umzusetzen (§ 27 Abs. 1 ZAG). Das heißt, es ist der Wesensart, dem Umfang und der Komplexität der mit der Tätigkeit des Instituts einhergehenden Risiken Rechnung zu tragen. Das Proportionalitätsprinzip knüpft also an die individuellen Risiken eines jeden Instituts an. Art und Umfang der erbrachten Zahlungsdienste sowie eine geringe Institutsgröße können Indikatoren für schwächer ausgeprägte Risiken sein - und umgekehrt.

5 Die Anwendung des Grundsatzes der Proportionalität wirkt sich darauf aus, wie Anforderungen erfüllt werden können. So können bei Instituten mit schwächer ausgeprägten Risiken einfachere Strukturen, IT-Systeme oder Prozesse ausreichend sein. Umgekehrt kann das Proportionalitätsprinzip bei Instituten mit stärker ausgeprägten Risiken aufwändigere Strukturen, IT-Systeme oder Prozesse erfordern.

6 Die Einschätzung, welche Gestaltung als proportional anzusehen ist, ist in Bezug auf das einzelne Institut nicht statisch, sondern passt sich im Zeitablauf den sich verändernden Gegebenheiten an. In diesem Sinne haben die Institute und Gruppen zu prüfen, ob und wie die vorhandenen Strukturen, IT-Systeme oder Prozesse weiterentwickelt werden können und ggf. müssen.

II. Anforderungen

1. IT-Strategie

1.1. Die Geschäftsleitung hat eine mit der Geschäftsstrategie konsistente IT-Strategie festzulegen, in der die Ziele sowie die Maßnahmen zur Erreichung dieser Ziele dargestellt werden. Die IT-Strategie ist durch die Geschäftsleitung regelmäßig und anlassbezogen zu überprüfen und erforderlichenfalls anzupassen. Die Geschäftsleitung muss für die Umsetzung der IT-Strategie Sorge tragen.

1.2. Mindestinhalte der IT-Strategie sind:

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

(b) die 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) die strategische Entwicklung der IT-Architektur

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

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. Informationsdienste, Telekommunikationsdienstleistungen, Versorgungsleistungen etc.). 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

	(f) Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen (Hardware- und Software-Komponenten)	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
1.3.	Die Geschäftsleitung hat einen Strategieprozess einzurichten, der sich insbesondere auf die Prozessschritte „Planung", „Umsetzung", „Beurteilung" und „Anpassung" der Strategien erstreckt. Die in der IT-Strategie niedergelegten Ziele sind so zu formulieren, dass eine sinnvolle Überprüfung der Zielerreichung möglich ist. Die Ursachen für etwaige Abweichungen sind zu analysieren.	
1.4.	Die IT-Strategie sowie ggf. erforderliche Anpassungen der IT-Strategie sind dem Aufsichtsorgan des Instituts zur Kenntnis zu geben und mit diesem zu erörtern.	
1.5.	Die Inhalte sowie Änderungen der IT-Strategie sind innerhalb des Instituts in geeigneter Weise zu kommunizieren.	

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 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.

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. 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 wesentlichen Auslagerungen.	.
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.	Die Mitarbeiter müssen fortlaufend - abhängig von ihren Aufgaben, Kompetenzen und Verantwortlichkeiten - über die erforderlichen Kenntnisse und Erfahrungen verfügen. Durch geeignete Maßnahmen ist zu gewährleisten, dass das Qualifikationsniveau der Mitarbeiter angemessen ist.	
2.5.	Die Abwesenheit oder das Ausscheiden von Mitarbeitern darf nicht zu nachhaltigen Störungen der Betriebsabläufe führen.	

2.6.	Interessenkonflikte und unvereinbare Tätigkeiten innerhalb der IT-Aufbau- und IT-Ablauforganisation sind zu vermeiden.	So soll bspw. bei der Ausgestaltung der IT-Aufbau- und IT-Ablauforganisation sichergestellt werden, dass miteinander unvereinbare Tätigkeiten durch unterschiedliche Mitarbeiter ausgeführt werden. Interessenkonflikten zwischen Aktivitäten, die bspw. 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.
2.7.	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, die Wartbarkeit, die Anpassbarkeit an neue Anforderungen, die Sicherheit der IT-Systeme oder der dazugehörigen IT-Prozesse sowie deren Kosten berücksichtigt werden.
2.8.	Umfang und Qualität der technisch-organisatorischen Ausstattung haben sich insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie der Risikosituation zu orientieren.	
2.9.	Die IT-Systeme (Hardware- und Software-Komponenten), die dazugehörigen IT-Prozesse und sonstige Bestandteile des Informationsverbunds 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. 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.	**Informationsverbund** Zu einem Informationsverbund gehören bspw. geschäftsrelevante Informationen, Geschäfts- und Unterstützungsprozesse, IT-Systeme, die zugehörigen IT-Prozesse sowie Netz- und Gebäudeinfrastrukturen. **Standards zur Ausgestaltung der IT-Systeme** Zu solchen Standards zählen z. B. der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI), die internationalen Sicherheitsstandards ISO/IEC 270XX der International Organization for Standardization und der Payment Card Industry Data Security Standard (PCI-

		DSS). Das Abstellen auf gängige Standards zielt nicht auf die Verwendung von Standardhardware bzw. -software ab. Eigenentwicklungen sind grundsätzlich ebenso möglich.

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 haben sich insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie an der Risikosituation zu orientieren. IT-Systeme, die zugehörigen IT-Prozesse und sonstigen Bestandteile des Informationsverbunds müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Das Institut hat die mit dem Management der Informationsrisiken verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege zu definieren und aufeinander abzustimmen. Hierfür hat das Institut angemessene Überwachungs- und Steuerungsprozesse einzurichten und diesbezügliche Berichtspflichten zu definieren.	
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 bspw. geschäftsrelevante Informationen, Geschäfts- und Unterstützungsprozesse, IT-Systeme und die zugehörigen IT-Prozesse sowie Netz- und Gebäudeinfrastrukturen. Abhängigkeiten und Schnittstellen berücksichtigen auch die Vernetzung des Informationsverbunds mit Dritten.

3.4.	Das Institut hat regelmäßig und anlassbezogen den Schutzbedarf für die Bestandteile seines definierten Informationsverbunds, 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 Schadenpotenzial, 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 Informationsverbunds, 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 die 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. Das Informationssicherheitsmanagement folgt einem fortlaufenden Prozess, der die Phasen „Planung“, „Umsetzung“, „Erfolgskontrolle“ sowie „Optimierung“ und „Verbesserung“ umfasst.	
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 prüfen 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, der 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 gehören 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 Informationssicherheitsrichtlinien 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.	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) • die 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 bezüglich der Informationssicherheitsbelange • die Realisierung von Informationssicherheitsmaßnahmen zu initiieren und zu überwachen • die Überwachung und Hinwirkung auf die 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 Interessenkonflikte zu vermeiden.	Zur Vermeidung möglicher Interessenkonflikte werden insbesondere folgende Maßnahmen beachtet: • Funktions- und Stellenbeschreibung für den Informationssicherheitsbeauftragten, seinen Vertreter und ggf. weitere Stellen • Festlegung der erforderlichen Ressourcenausstattung für die Funktion des Informationssicherheitsbeauftragten

		• ein der Funktion zugewiesenes Budget für Informationssicherheitsschulungen 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.	Institute können die Funktion des Informationssicherheitsbeauftragten grundsätzlich mit anderen Funktionen im Institut kombinieren. Nur in folgenden Fällen kann der Informationssicherheitsbeauftragte außerhalb des Instituts angesiedelt werden: Institute mit geringer Mitarbeiteranzahl, geringem Informationsrisiko und ohne wesentliche eigen betriebene IT, bei denen die IT-Dienstleistungen im Wesentlichen durch einen externen IT-Dienstleister erbracht werden, können die Funktion des Informationssicherheitsbeauftragten auf einen fachlich qualifizierten Dritten übertragen. Konzernangehörige Institute mit geringer Mitarbeiteranzahl, geringem Informationsrisiko und ohne wesentliche eigen betriebene IT, bei denen IT-Dienstleistungen im Wesentlichen durch konzernangehörige Unternehmen

		erbracht werden, können die Funktion des Informationssicherheitsbeauftragten auch auf den Informationssicherheitsbeauftragten eines Konzernunternehmens übertragen. In beiden Fällen ist im Institut eine interne Ansprechperson für den Informationssicherheitsbeauftragten zu benennen. 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 Begriffs „Informationssicherheitsvorfall" nach Art und Umfang orientiert sich am Schutzbedarf der betroffenen Bestandteile des Informationsverbunds. 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 diese regelmäßig und anlassbezogen zu überprüfen und bei Bedarf anzupassen.	Die Richtlinie berücksichtigt u. a.: • die allgemeine Bedrohungslage • die individuelle Risikosituation des Instituts • Kategorien von Test- und Überprüfungsobjekten (z. B. Institut, IT-Systeme, Komponenten) • die Art, der Umfang und die 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 bspw. 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 sonstigen Bestandteile des Informationsverbunds müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Für IT-Risiken sind angemessene Überwachungs- und Steuerungsprozesse einzurichten, die insbesondere die Festlegung von IT-Risikokriterien, die Identifikation von IT-Risiken, die Festlegung des Schutzbedarfs, daraus abgeleitete Schutzmaßnahmen für den IT-Betrieb sowie die Festlegung entsprechender Maßnahmen zur Risikobehandlung und -minderung umfassen.	

5.2.	Das 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.: • das Schwachstellenmanagement zur Erkennung, Bewertung, Behandlung und Dokumentation von Schwachstellen • die Segmentierung und die Kontrolle des Netzwerks (einschließlich Richtlinienkonformität der Endgeräte) • die sichere Konfiguration von IT-Systemen (Härtung) • die Verschlüsselung von Daten bei Speicherung und Übertragung gemäß Schutzbedarf • den mehrstufigen Schutz der IT-Systeme gemäß Schutzbedarf (z. B. vor Datenverlust, Manipulation, Verfügbarkeitsangriffe oder vor nicht autorisiertem Zugriff) • den Perimeterschutz von z. B. Liegenschaften, Rechenzentren und anderen sensiblen Bereichen.
5.3.	Gefährdungen des Informationsverbunds sind möglichst frühzeitig zu identifizieren. Potenziell 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.	Potenziell 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 Mustern) 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 bspw., 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 bspw. aus der regelbasierten Auswertung der potenziell sicherheitsrelevanten Informationen. Die zeitnahe Analyse und Reaktion können 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 Interessenkonflikten zu überprüfen. Ergebnisse sind hinsichtlich notwendiger Verbesserungen zu analysieren und Risiken sind angemessen zu steuern.	Turnus, Art und Umfang der Überprüfung sollten sich insbesondere am Schutzbedarf und der potenziellen Angriffsfläche (z. B. Erreichbarkeit aus dem Internet) des IT-Systems orientieren. Arten der Überprüfungen sind z. B.: • Abweichungsanalysen (Gap-Analyse) • Schwachstellenscans • Penetrationstests • Simulationen von Angriffen.

6. Identitäts- und Rechtemanagement

6.1.	Das Institut hat ein Identitäts- und Rechtemanagement einzurichten, welches sicherstellt, dass den Benutzern eingeräumte Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben des Instituts entspricht. Bei der Ausgestaltung des Identi-	

	täts- und Rechtemanagements sind die Anforderungen an die Ausgestaltung der Prozesse (siehe Tzn. 2.2., 2.6. und 2.9.) entsprechend zu berücksichtigen. Jegliche Zugriffs-, Zugangs- und Zutrittsrechte auf Bestandteile bzw. zu Bestandteilen des Informationsverbunds 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 Interessenkonflikte 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. 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.
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 umfasst 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.	Berechtigungen sind bei Bedarf zeitnah anzupassen. Dies beinhaltet auch die regelmäßige und anlassbezogene Überprüfung innerhalb angemessener Fristen, ob die eingeräumten Berechtigungen weiterhin benötigt werden und ob diese den Vorgaben des Berechtigungskonzepts entsprechen (Rezertifizierung). Bei der Rezertifizierung sind die für die Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen zuständigen Kontrollinstanzen einzubeziehen. Wesentliche Berechtigungen sind mindestens jährlich zu überprüfen, alle anderen mindestens alle drei Jahre. Besonders kritische Berechtigungen, wie sie bspw. Administratoren aufweisen, sind mindestens halbjährlich zu überprüfen.	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-/ 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 bspw.: • die Auswahl angemessener Authentifizierungsverfahren (u. a. starke Authentifizierung im Falle von Fernzugriffen) • die Implementierung einer Richtlinie zur Wahl sicherer Passwörter • die automatische passwortgesicherte Bildschirmsperre • die Verschlüsselung von Daten • die manipulationssichere Implementierung der Protokollierung • die 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 vorab im Rahmen einer Auswirkungsanalyse zu bewerten. Dabei hat das Institut insbesondere die Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität zu analysieren. In diesen Analysen sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten zu beteiligen. Dies gilt auch im Hinblick auf den erstmaligen Einsatz sowie wesentliche Veränderungen von IT-Systemen.

7.2.	Die organisatorischen Grundlagen für IT-Projekte und die Kriterien für deren Anwendung sind zu regeln.	Organisatorische Grundlagen berücksichtigen u. a.: • die Einbindung betroffener Beteiligter (insbesondere des Informationssicherheitsbeauftragten) • die Projektdokumentation (z. B. Projektantrag, Projektabschlussbericht) • die quantitative und qualitative Ressourcenausstattung • die Steuerung der Projektrisiken • die Informationssicherheitsanforderungen • projektunabhängige Qualitätssicherungsmaßnahmen • die Aufarbeitung der gewonnenen Erkenntnisse (Lessons Learned).
7.3.	IT-Projekte sind angemessen unter Berücksichtigung ihrer Ziele und Risiken im Hinblick auf die Dauer, die Ressourcen und die 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.	Die 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 Anforderungen (funktional und nicht funktional) haben die fachlich verantwortlichen Stellen zu tragen.	Anforderungsdokumente können sich je nach Vorgehensmodell unterscheiden und beinhalten bspw.: • Fachkonzept (Lastenheft) • Technisches Fachkonzept (Pflichtenheft) • User-Story/Product Back-Log Nichtfunktionale Anforderungen an IT-Systeme sind bspw.: • 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,	Geeignete Vorkehrungen sind z. B.: • Prüfung der Eingabedaten • Systemzugangskontrolle

	Verfügbarkeit und Authentizität der zu verarbeitenden Daten nachvollziehbar sichergestellt werden.	• 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 bspw. eine Versionierung des Quellcodes und der Anforderungsdokumente bei.

7.11.	Die IT-Systeme sind vor ihrem erstmaligen Einsatz und nach wesentlichen Veränderungen 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.	Bei der Beurteilung der Wesentlichkeit von Veränderungen ist nicht auf den Umfang der Veränderungen, sondern auf die Auswirkungen, die eine Veränderung auf die Funktionsfähigkeit des betroffenen IT-Systems haben kann, abzustellen. Bei der Abnahme durch die fachlich und die technisch zuständigen Mitarbeiter stehen die Eignung und Angemessenheit der IT-Systeme für die spezifische Situation des jeweiligen Instituts im Mittelpunkt. Gegebenenfalls vorliegende Testate Dritter können bei der Abnahme berücksichtigt werden, sie können die Abnahme jedoch nicht vollständig ersetzen.
7.12.	Es ist eine Methodik für das Testen von Anwendungen vor deren erstmaligem 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 den für den Test wesentlichen Aspekten der Produktionsumgebung zu entsprechen. Testaktivitäten und Testergebnisse sind zu dokumentieren.	Die Testdurchführung erfordert eine einschlägige Expertise der Tester sowie eine angemessen ausgestaltete Unabhängigkeit von den Anwendungsentwicklern. Der Schutzbedarf der zum Test verwendeten Daten ist zu berücksichtigen. Eine Testdokumentation enthält mindestens folgende Punkte: • Testfallbeschreibung • Dokumentation der zugrunde gelegten Parametrisierung des Testfalls • Testdaten • Erwartetes Testergebnis • Erzieltes Testergebnis • Aus den Tests abgeleitete Maßnahmen. Risikoorientiert schließen die Maßnahmen zum Schutz der Informationen auch Penetrationstests ein.

7.13.	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.
7.14.	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 Anwendung, werden Schutzmaßnahmen in Abhängigkeit der Ergebnisse der Schutzbedarfsklassifizierung ergriffen.
7.15.	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. Tzn. 2.8. und 2.9.).	
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 Patch-Level) • 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).	Die 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 an einen 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 bspw.: • Risikoanalysen 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 bspw. 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 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 um angemessen reagieren zu können. Bei der Planung sind Leistungs- und Kapazitätsbedarf von Informationssicherheitsmaßnahmen zu berücksichtigen.	

9. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

Der Abschnitt 9. bezieht sich ausschließlich auf Auslagerungen von IT-Aktivitäten und IT-Prozessen sowie den sonstigen Fremdbezug von IT-Dienstleistungen.

9.1.	Grundsätzlich sind IT-Aktivitäten und IT-Prozesse auslagerbar, solange dadurch die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 27 ZAG nicht beeinträchtigt wird. Die Auslagerung von IT-Akti-	**Befugnis der Leistungserbringung des Auslagerungsunternehmens** Durch das Institut ist sicherzustellen, dass das Auslagerungsunternehmen nach dem Recht seines Sitzlands zur Ausübung der ausgelagerten Aktivitäten und Prozesse befugt ist und über dazu ggf. erforderliche Erlaubnisse und

	vitäten und IT-Prozessen darf nicht zu einer Delegation der Verantwortung der Geschäftsleitung an das Auslagerungsunternehmen führen. Die Leitungsaufgaben der Geschäftsleitung sind nicht auslagerbar. Auslagerungen dürfen nicht dazu führen, dass das Institut nur noch als leere Hülle (empty shell) existiert.	Registrierungen verfügt. Bei Auslagerungen an Unternehmen mit Sitz außerhalb des Europäischen Wirtschaftsraums (EWR) hat das Institut, sofern es sich um ausgelagerte Aktivitäten oder Prozesse von Zahlungsdiensten in einem Umfang handelt, der innerhalb des EWR eine Zulassung oder Registrierung durch die zuständigen Aufsichtsbehörden erfordern würde, ferner sicherzustellen, dass das Auslagerungsunternehmen von den zuständigen Aufsichtsbehörden in dem Drittstaat beaufsichtigt wird und eine entsprechende Kooperationsvereinbarung, z. B. in Form einer Absichtserklärung („Memorandum of Understanding“) oder College-Vereinbarung zwischen den für die Beaufsichtigung des Instituts zuständigen Aufsichtsbehörden und den für die Beaufsichtigung des Auslagerungsunternehmens zuständigen Aufsichtsbehörden besteht.
9.2.	IT-Dienstleistungen umfassen alle Ausprägungen des Bezugs von IT; dazu zählen insbesondere die Bereitstellung von IT-Systemen, Projekten oder anderen Personaldienstleistungen. Hierzu zählen auch IT-Dienstleistungen, die durch ein Dienstleistungsunternehmen über ein Netz bereitgestellt werden (z. B. Rechenleistung, Speicherplatz, Plattformen oder Software) und deren Angebot, Nutzung und Abrechnung ggf. dynamisch und an den Bedarf angepasst über definierte technische Schnittstellen sowie Protokolle erfolgen (Cloud-Dienstleistungen). Bei der Auslagerung von IT-Aktivitäten und IT-Prozessen hat das Institut die Vorgaben gemäß § 26 ZAG zu beachten. Beim sonstigen Fremdbezug von IT-Dienstleistungen haben die Institute die allgemeinen Anforderungen an die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 27 ZAG zu beachten. Bei jedem Bezug von Hard- und Software sind die damit verbundenen Risiken angemessen zu bewerten.	

9.3. Eine Auslagerung von IT-Aktivitäten und IT-Prozessen in Kontrollbereichen und Kerninstitutsbereichen kann unter Beachtung der in Tz. 9.1. genannten Anforderungen in einem Umfang vorgenommen werden, der gewährleistet, dass hierdurch das Institut weiterhin über Kenntnisse und Erfahrungen verfügt, die eine wirksame Überwachung der vom Auslagerungsunternehmen erbrachten IT-Dienstleistungen gewährleistet. Es ist sicherzustellen, dass bei Bedarf - im Falle der Beendigung des Auslagerungsverhältnisses oder der Änderung der Gruppenstruktur - der ordnungsmäßige Betrieb in diesen Bereichen fortgesetzt werden kann.

9.4. Eine Auslagerung liegt vor, wenn ein anderes Unternehmen mit der Wahrnehmung von IT-Aktivitäten oder IT-Prozessen, die für die Durchführung von Zahlungsdiensten, E-Geld-Geschäft oder sonstigen institutstypischen Dienstleistungen beauftragt wird, die ansonsten vom Institut selbst erbracht würden. Zivilrechtliche Gestaltungen und Vereinbarungen können dabei das Vorliegen einer Auslagerung nicht von vornherein ausschließen.

Sonstiger Fremdbezug von IT-Dienstleistungen

Nicht als Auslagerung im Sinne dieses Rundschreibens zu qualifizieren ist der sonstige Fremdbezug von IT-Dienstleistungen. Hierzu zählt in der Regel der isolierte Bezug von Hard- und Software. Hierzu gehören u. a. auch die folgenden Unterstützungsleistungen:

- die Anpassung der Software an die Erfordernisse des Instituts
- 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 (Wartung) gemäß der Anforderungs-/Fehlerbeschreibung des Auftraggebers oder Herstellers
- sonstige Unterstützungsleistungen, die über die reine Beratung hinausgehen.

		Dies gilt nicht für Software, die zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation der Risiken eingesetzt wird oder die für die Durchführung von zahlungsdienstegeschäftlichen Aufgaben von wesentlicher Bedeutung ist; bei dieser Software sind Unterstützungsleistungen als Auslagerung einzustufen. Die gleichen Maßstäbe gelten für den Betrieb der Software durch einen externen Dritten.
9.5.	Das Institut muss anhand einer Risikoanalyse vorab bewerten, welche Risiken mit einer Auslagerung von IT-Aktivitäten und IT-Prozessen bzw. dem Fremdbezug von IT-Dienstleistungen verbunden sind. Ausgehend von dieser Risikoanalyse ist eigenverantwortlich festzulegen, welche Auslagerungen von IT-Aktivitäten und IT-Prozessen unter Risikogesichtspunkten wesentlich sind (wesentliche Auslagerungen). Diese ist auf der Grundlage von institutsweit bzw. gruppenweit einheitlichen Rahmenvorgaben sowohl regelmäßig als auch anlassbezogen durchzuführen. Die Ergebnisse der Risikoanalyse sind in der Auslagerungs- und Risikosteuerung zu beachten. Die maßgeblichen Organisationseinheiten sind bei der Erstellung der Risikoanalyse einzubeziehen. Im Rahmen ihrer Aufgaben ist auch die Interne Revision zu beteiligen.	Bei der Risikoanalyse sind alle für das Institut relevanten Aspekte im Zusammenhang mit der Auslagerung von IT-Aktivitäten und IT-Prozessen oder dem sonstigen Fremdbezug von IT-Dienstleistungen zu berücksichtigen (z. B. die wesentlichen Risiken einschließlich möglicher Risikokonzentrationen (u. a. mehrere Auslagerungsvereinbarungen bzw. Auslagerungsverträge mit demselben Auslagerungsunternehmen), Risiken aus Weiterverlagerungen, politische Risiken, Maßnahmen zur Steuerung und Minderung der Risiken, Eignung des Auslagerungsunternehmens, mögliche Interessenkonflikte, Schutzbedarf der an das Auslagerungsunternehmen übermittelten Daten, Kosten), wobei die Intensität der Analyse von Art, Umfang, Komplexität und Risikogehalt der ausgelagerten IT-Aktivitäten und IT-Prozessen abhängt. Insbesondere ist in der Risikoanalyse zu berücksichtigen, inwiefern eine auszulagernde IT-Aktivität oder ein auszulagernder IT-Prozess innerhalb der Prozesslandschaft des Instituts als wesentlich einzustufen ist. Bei Auslagerungen von IT-Aktivitäten oder IT-Prozessen mit erheblicher Tragweite ist entsprechend intensiv zu prüfen, ob und wie eine Einbeziehung der ausgelagerten IT-Aktivitäten und IT-Prozesse in das Risikomanagement sichergestellt werden kann. Art und Umfang einer Risikoanalyse kann das Institut unter Proportionalitätsgesichtspunkten nach Maßgabe seines allgemeinen Risikomanagements flexibel festlegen. Für gleichartige Formen des sonstigen Fremdbezugs von

		IT-Dienstleistungen kann auf bestehende Risikoanalysen zurückgegriffen werden. Die für Informationssicherheit und Notfallmanagement verantwortlichen Funktionen des Instituts werden eingebunden.
9.6.	Die Risikoanalysen für die Auslagerungen von IT-Aktivitäten und IT-Prozessen sowie dem sonstigen Fremdbezug von IT-Dienstleistungen sind regelmäßig und anlassbezogen zu überprüfen und ggf. inkl. der Vertragsinhalte anzupassen.	
9.7.	Die Auslagerungen von IT-Aktivitäten und IT-Prozessen und der sonstige Fremdbezug von IT-Dienstleistungen sind im Einklang mit den Strategien unter Berücksichtigung der Risikoanalyse des Instituts zu steuern. Die Erbringung der vom Dienstleister geschuldeten Leistung ist entsprechend der Risikoanalyse zu überwachen.	
9.8.	Bei der Vertragsgestaltung sind die aus den Risikoanalysen abgeleiteten Maßnahmen angemessen 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 bspw. 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.
9.9.	Das Institut hat bei wesentlichen Auslagerungen von IT-Aktivitäten oder IT-Prozessen im Fall der beabsichtigten oder erwarteten Beendigung der Auslagerungsvereinbarung Vorkehrungen zu treffen, um die	Ausstiegsprozesse sind mit dem Ziel festzulegen, die notwendige Kontinuität und Qualität der ausgelagerten IT-Aktivitäten und IT-Prozesse aufrechtzuerhalten bzw. in angemessener Zeit wieder herstellen zu können.

	Kontinuität und Qualität der ausgelagerten IT-Aktivitäten und IT-Prozesse auch nach Beendigung zu gewährleisten. Für Fälle unbeabsichtigter oder unerwarteter Beendigung dieser Auslagerungen, die mit einer erheblichen Beeinträchtigung der Geschäftstätigkeit verbunden sein können, hat das Institut etwaige Handlungsoptionen auf deren Durchführbarkeit zu prüfen und zu verabschieden. Dies beinhaltet auch, soweit sinnvoll und möglich, die Festlegung entsprechender Ausstiegsprozesse. Die Handlungsoptionen sind regelmäßig und anlassbezogen zu überprüfen.	Existieren keine Handlungsoptionen, ist zumindest eine angemessene Berücksichtigung in der Notfallplanung erforderlich.
9.10.	Bei wesentlichen Auslagerungen von IT-Aktivitäten und IT-Prozessen ist im schriftlichen Auslagerungsvertrag insbesondere Folgendes zu vereinbaren: (a) Spezifizierung und ggf. Abgrenzung der vom Auslagerungsunternehmen zu erbringenden Leistung (b) Datum des Beginns und ggf. des Endes der Auslagerungsvereinbarung (c) sofern vom deutschen Recht abweichendes Recht für die Auslagerungsvereinbarung gelten soll (d) Standorte (d.h. Regionen und Länder), in denen die Durchführung der Dienstleistung erfolgt und/oder maßgebliche Daten gespeichert und verarbeitet werden, sowie die Regelung, dass das Institut benachrichtigt wird, wenn das Auslagerungsunternehmen den Standort wechselt (e) vereinbarte Dienstleistungsgüte mit eindeutig festgelegten Leistungszielen	**Weisungsrechte des Instituts/Prüfungen der Internen Revision** Auf eine explizite Vereinbarung von Weisungsrechten zugunsten des Instituts kann verzichtet werden, wenn die vom Auslagerungsunternehmen zu erbringende Leistung hinreichend klar im Auslagerungsvertrag spezifiziert ist. Ferner kann die Interne Revision des auslagernden Instituts von eigenen Prüfungshandlungen absehen, sofern eine anderweitig durchgeführte Revisionstätigkeit, z. B. in Form von Group-Audits den aufsichtlichen Anforderungen genügt. Diese Erleichterungen können auch bei Auslagerungen auf so genannte Mehrmandantendienstleister in Anspruch genommen werden. **Informations- und Prüfungsrechte** Durch eine Auslagerung von IT-Aktivitäten und IT-Prozessen darf die Bundesanstalt an der Wahrnehmung ihrer Aufgaben nicht gehindert werden; ihre Auskunfts- und Prüfungsrechte sowie Kontrollmöglichkeiten müssen in Bezug auf die ausgelagerten IT-Aktivitäten und IT-Prozesse auch bei einer

(f) soweit zutreffend, dass das Auslagerungsunternehmen für bestimmte Risiken einen Versicherungsnachweis vorzulegen hat

(g) Anforderungen für die Umsetzung und Überprüfung von Notfallkonzepten

(h) Festlegung angemessener Informations- und Prüfungsrechte der Internen Revision sowie externer Prüfer

(i) Sicherstellung der uneingeschränkten Informations- und Prüfungsrechte sowie der Kontrollmöglichkeiten der gemäß § 26 ZAG zuständigen Behörden bezüglich der ausgelagerten IT-Aktivitäten und IT-Prozesse

(j) soweit erforderlich Weisungsrechte

(k) Regelungen, die sicherstellen, dass datenschutzrechtliche Bestimmungen und sonstige Sicherheitsanforderungen beachtet werden

(l) Kündigungsrechte und angemessene Kündigungsfristen

(m) Regelungen über die Möglichkeit und über die Modalitäten einer Weiterverlagerung, die sicherstellen, dass das Institut die bankaufsichtsrechtlichen Anforderungen weiterhin einhält und

(n) Verpflichtung des Auslagerungsunternehmens, das Institut über Entwicklungen zu informieren, die die ordnungsgemäße Erledigung der ausgelagerten IT-Aktivitäten und IT-Prozesse beeinträchtigen können.

Auslagerung auf ein Unternehmen mit Sitz im Ausland durch geeignete Vorkehrungen gewährleistet werden; Entsprechendes gilt für die Wahrnehmung der Aufgaben der Prüfer des Instituts.

Informations- und Prüfungsrechte sollten möglichst auch für nicht wesentliche Auslagerungen von IT-Aktivitäten und IT-Prozessen vereinbart werden, sofern abzusehen ist, dass diese Auslagerungen in naher oder mittlerer Zukunft wesentlich werden könnten.

Die Informations- und Prüfungsrechte umfassen auch die für den Zutritt, Zugang oder Zugriff erforderlichen Rechte.

Eskalation bei Schlechtleistung

Bereits bei der Vertragsanbahnung hat das Institut intern festzulegen, welchen Grad einer Schlechtleistung es akzeptieren möchte.

Kündigungsrechte

Die Auslagerungsvereinbarung sollte das Auslagerungsunternehmen für den Fall einer Kündigung verpflichten, das Institut bei der Übertragung der ausgelagerten IT-Aktivität bzw. des ausgelagerten IT-Prozesses an ein anderes Auslagerungsunternehmen oder ihre bzw. seine Reintegration in das Institut zu unterstützen.

Sonstige Sicherheitsanforderungen

Regelungen zu sonstigen Sicherheitsanforderungen sollten für alle, also auch nicht wesentliche Auslagerungen, vertraglich vereinbart werden.

Zu den sonstigen Sicherheitsanforderungen zählen vor allem Zugangsbestimmungen zu Räumen und Gebäuden (z. B. bei Rechenzentren) sowie Zugriffsberechtigungen auf Softwarelösungen zum Schutz wesentlicher Daten und Informationen. Die Einhaltung dieser Anforderungen ist fortlaufend zu überwachen.
Institute sollten einen risikobasierten Ansatz betreffend den Standort der Datenspeicherung und Datenverarbeitung sowie hinsichtlich der Informationssicherheit wählen. Es ist sicherzustellen, dass auf die sich im Eigentum des Instituts befindlichen Daten im Fall einer Insolvenz, Abwicklung oder der Einstellung der Geschäftstätigkeit des Auslagerungsunternehmens zugegriffen werden kann.

Ort der Durchführung der Dienstleistung
Zusätzlich zu Tz. 9.10 d) muss der Ort der Leistungserbringung (z. B. Stadt oder sofern notwendig genaue Anschrift) dem Institut jederzeit bekannt sein.

9.11. Mit Blick auf Weiterverlagerungen sind möglichst Zustimmungsvorbehalte des auslagernden Instituts oder konkrete Voraussetzungen, wann Weiterverlagerungen einzelner Arbeits- und Prozessschritte möglich sind, im Auslagerungsvertrag zu vereinbaren. Zumindest ist vertraglich sicherzustellen, dass die Vereinbarungen des Auslagerungsunternehmens mit Subunternehmen im Einklang mit den vertraglichen Vereinbarungen des originären Auslagerungsvertrags stehen. Ferner haben die vertraglichen Anforderungen bei Weiterverlagerungen auch eine Informationspflicht des Auslagerungsunternehmens an das auslagernde Institut zu umfassen. Es muss sichergestellt

sein, dass das Auslagerungsunternehmen im Falle einer Weiterverlagerung auf ein Subunternehmen weiterhin gegenüber dem auslagernden Institut berichtspflichtig bleibt.

Das Institut hat die mit Auslagerungen von IT-Aktivitäten und IT-Prozessen verbundenen Risiken angemessen zu steuern und die Ausführung der ausgelagerten IT-Aktivitäten und IT-Prozesse ordnungsgemäß zu überwachen. Dies umfasst auch die laufende Überwachung der Leistung des Auslagerungsunternehmens anhand vorzuhaltender Kriterien (z. B. Key Performance Indicators, Key Risk Indicators) und vertraglich vereinbarter Informationen des Auslagerungsunternehmens. Die Qualität der erbrachten Leistungen ist regelmäßig zu beurteilen.

Die Anforderungen an die Auslagerung von IT-Aktivitäten und IT-Prozessen sind auch bei der Weiterverlagerung ausgelagerter IT-Aktivitäten und IT-Prozesse zu beachten.

9.12. Jedes Institut, das Auslagerungen von IT-Aktivitäten und IT-Prozessen vornimmt, hat einen zentralen Auslagerungsbeauftragten im Institut selbst einzurichten. Zusätzlich hat das Institut abhängig von der Art, dem Umfang und der Komplexität der Auslagerungsaktivitäten ein zentrales Auslagerungsmanagement zur Unterstützung des Auslagerungsbeauftragten einzurichten. Zu den Aufgaben zählen insbesondere:

(a) Implementierung und Weiterentwicklung eines angemessenen Auslagerungsmanagements und entsprechender Kontroll- und Überwachungsprozesse

Zentraler Auslagerungsbeauftragter

Der zentrale Auslagerungsbeauftragte hat einer Organisationseinheit anzugehören, die der Geschäftsleitung unmittelbar unterstellt ist.

Kleinere, weniger komplexe Institute können diese Funktion auch einem Mitglied der Geschäftsleitung übertragen.

Als Auslagerungsbeauftragter kann auch der Leiter des zentralen Auslagerungsmanagements benannt werden, sofern dieser die Anforderungen der Tz. 9.12. erfüllt.

(b) Erstellung und Pflege einer vollständigen Dokumentation der Auslagerungen (einschließlich Weiterverlagerungen)

(c) Unterstützung der Fachbereiche bezüglich der institutsinternen und gesetzlichen Anforderungen bei Auslagerungen

(d) Koordination und Überprüfung der durch die zuständigen Bereiche durchgeführten Risikoanalyse.

9.13. Der Auslagerungsbeauftragte bzw. das zentrale Auslagerungsmanagement hat mindestens jährlich sowie anlassbezogen einen Bericht über die wesentlichen Auslagerungen von IT-Aktivitäten und IT-Prozessen zu erstellen und der Geschäftsleitung zur Verfügung zu stellen. Der Bericht hat unter Berücksichtigung der dem Institut vorliegenden Informationen bzw. der institutsinternen Bewertung der Dienstleistungsqualität der Auslagerungsunternehmen eine Aussage darüber zu treffen, ob die erbrachten Dienstleistungen der Auslagerungsunternehmen den vertraglichen Vereinbarungen entsprechen, die ausgelagerten IT-Aktivitäten und IT-Prozesse angemessen gesteuert und überwacht werden können und ob weitere risikomindernde Maßnahmen ergriffen werden sollen.

Berichterstattung bei kleineren, weniger komplexen Instituten

Bei kleineren, weniger komplexen Instituten ist eine Berichterstattung im Rahmen einer Vorstandssitzung ausreichend.

9.14. Im Hinblick auf Gruppen im Sinne von § 1 Abs. 6 ZAG oder Finanzverbünde ergeben sich die folgenden Erleichterungen:

(a) Bei gruppen- und verbundinternen Auslagerungen von IT-Aktivitäten und IT-Prozessen können im Rahmen der Risikoanalyse wirksame Vorkehrungen auf Gruppenebene, insbesondere ein

Gemeinsame Notfallkonzepte

Wenn sich die Institute innerhalb einer Institutsgruppe oder eines Finanzverbundes auf ein gemeinsames Notfallkonzept für eine wesentliche Auslagerung geeinigt haben, haben die Institute den für sie relevanten Teil des Notfallkonzepts zu erhalten.

einheitliches und umfassendes Risikomanagement sowie Durchgriffsrechte, bei der Erstellung und Anpassung der Risikoanalyse risikomindernd berücksichtigt werden.

(b) Für Auslagerungen mehrerer Institute einer Gruppe bzw. eines Verbunds an ein bzw. mehrere gemeinsame Auslagerungsunternehmen besteht die Möglichkeit, ein zentrales Auslagerungsmanagement auf Gruppen- bzw. Verbundebene einzurichten, sofern das zentrale Auslagerungsmanagement den Anforderungen des Abschnitts 9. dieses Rundschreibens bzw. den Anforderungen der EBA GL 2019/02 genügt.

(c) Bei der Risikoberichterstattung von Auslagerungsunternehmen, die innerhalb einer Gruppe/eines Verbunds genutzt werden, besteht die Möglichkeit einer zentralen Vorauswertung, welche den auslagernden Instituten die weitere Verwendung erleichtert.

(d) Bei gruppen- und verbundinternen Auslagerungen von IT-Aktivitäten und IT-Prozesse kann auf die Erstellung von Ausstiegsprozessen und Handlungsoptionen verzichtet werden.

(e) Wird gruppen- oder verbundintern ein zentrales Auslagerungsregister eingerichtet und geführt, so muss sichergestellt sein, dass das einzelne Institut und die zuständige Behörde das individuelle Auslagerungsregister bei Bedarf ohne größere Verzögerung erhalten.

Auch für Auslagerungen von IT-Aktivitäten und IT-Prozessen innerhalb einer Institutsgruppe oder eines Finanzverbunds an ein zentrales Auslagerungsunternehmen innerhalb der Gruppe bzw. des Verbunds sind die Bedingungen, einschließlich der finanziellen Bedingungen, festzulegen.

9.15. Grundsätzlich hat das Institut ein aktuelles Auslagerungsregister mit Informationen über alle Auslagerungsvereinbarungen vorzuhalten. Die inhaltlichen Mindestanforderungen an das Auslagerungsregister finden sich für alle Auslagerungen in Tz. 54 und für wesentliche Auslagerungen in Tz. 55 der EBA-Leitlinien zu Auslagerungen (EBA/GL/2019/02). Das Auslagerungsregister umfasst alle Auslagerungsvereinbarungen, einschließlich der Auslagerungsvereinbarungen mit Auslagerungsunternehmen innerhalb einer Institutsgruppe oder eines Finanzverbunds. Ferner ist bei der Weiterverlagerung von wesentlichen Auslagerungen von dem auslagernden Institut festzulegen, ob der weiter zu verlagernde Teil wesentlich ist und dieser wesentliche Teil im Auslagerungsregister zu erfassen ist.

10. 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). Zeitkritisch sind grundsätzlich jene Aktivitäten und Prozesse, bei deren Beeinträchtigung für definierte Zeiträume ein nicht mehr akzeptabler Schaden für das Institut zu erwarten ist. Die Wirksamkeit und Angemessenheit des Notfallkonzepts sind regelmäßig zu überprüfen. Für zeitkritische Aktivitäten und Prozesse sind sie für alle relevanten Szenarien mindestens jährlich und anlassbezogen nachzuweisen.

10.2. Zur Identifikation von zeitkritischen Aktivitäten und Prozessen sowie von unterstützenden Aktivitäten und Prozessen, hierfür notwendigen IT-Systemen und sonstigen notwendigen Ressourcen sowie der Als Basis für die Auswirkungsanalysen dient eine Übersicht über alle Aktivitäten und Prozesse (z. B. in Form einer Prozesslandkarte).

	potenziellen Gefährdungen hat das Institut Auswirkungsanalysen und Risikoanalysen durchzuführen.	**Auswirkungsanalysen** In Auswirkungsanalysen wird über abgestufte Zeiträume betrachtet, welche Folgen eine Beeinträchtigung von Aktivitäten und Prozessen für den Geschäftsbetrieb haben kann. Die Auswirkungsanalysen sollten u. a. folgende Aspekte berücksichtigen: • Art und Umfang des (im-)materiellen Schadens • Zeitpunkt des Ausfalls **Risikoanalysen** In Risikoanalysen für die identifizierten, zeitkritischen Aktivitäten und Prozesse werden potenzielle Gefährdungen identifiziert und bewertet, welche eine Beeinträchtigung der zeitkritischen Geschäftsprozesse verursachen können.
10.3.	Die im Notfallkonzept festgelegten Maßnahmen müssen dazu geeignet sein, das Ausmaß möglicher Schäden zu reduzieren. Das Notfallkonzept muss Geschäftsfortführungs- sowie Wiederherstellungspläne umfassen. Geschäftsfortführungspläne müssen gewährleisten, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen. Wiederherstellungspläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen. Bei Notfällen ist eine angemessene interne und externe Kommunikation sicherzustellen. Im Fall der Auslagerung von zeitkritischen Aktivitäten und Prozessen haben das auslagernde Institut und das Auslagerungsunternehmen über aufeinander abgestimmte Notfallkonzepte zu verfügen.	Im Notfallkonzept werden Verantwortlichkeiten, Ziele und Maßnahmen zur Fortführung bzw. Wiederherstellung von zeitkritischen Aktivitäten und Prozessen bestimmt und Kriterien für die Einstufung sowie für das Auslösen der Pläne definiert. Hierbei werden mindestens folgende Szenarien berücksichtigt: • (Teil-)Ausfall eines Standorts (z. B. durch Hochwasser, Großbrand, Gebietssperrung, Ausfall der Zutrittskontrolle) • erheblicher Ausfall von IT-Systemen oder Kommunikationsinfrastruktur (z. B. aufgrund von Fehlern oder Angriffen) • Ausfall einer kritischen Anzahl von Mitarbeitern (z. B. bei Pandemie, Lebensmittelvergiftung, Streik)

	Das Notfallkonzept ist anlassbezogen zu aktualisieren, jährlich auf Aktualität zu überprüfen und angemessen zu kommunizieren.	• Ausfall von Dienstleistern (z. B. Zulieferer, Stromversorger).
10.4.	Die Wirksamkeit und Angemessenheit des Notfallkonzepts sind regelmäßig zu überprüfen. Für zeitkritische Aktivitäten und Prozesse ist dies für alle relevanten Szenarien mindestens jährlich und anlassbezogen nachzuweisen. Überprüfungen des Notfallkonzepts sind zu protokollieren. Ergebnisse sind hinsichtlich notwendiger Verbesserungen zu analysieren, Risiken sind angemessen zu steuern. Die Ergebnisse sind den jeweiligen Verantwortlichen schriftlich mitzuteilen.	Die Häufigkeit und der Umfang der Überprüfungen sollten sich grundsätzlich an der Gefährdungslage orientieren. Dienstleister sind angemessen einzubinden. Überprüfungen beinhalten u. a.: • Test der technischen Vorsorgemaßnahmen • Kommunikations-, Krisenstabs- und Alarmierungsübungen • Ernstfall- oder Vollübungen
10.5.	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).
10.6.	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 IT-Systeme • Notwendige Ressourcen, um eine (eingeschränkte) Fortführung der Geschäftsprozesse zu gewährleisten • Abhängigkeiten von externen Faktoren (Gesetzgeber, Anteilseigner, Öffentlichkeit etc.).
10.7.	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).
10.8.	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.	

10.9.	Die Geschäftsleitung hat sich mindestens quartalsweise und anlassbezogen über den Zustand des Notfallmanagements schriftlich berichten zu lassen.	

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 ZAIT und den sonstigen einschlägigen zahlungsdiensteaufsichtlichen 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 zahlungsdienstaufsichtlichen 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.

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

12.2.	Der Geltungsbereich der kritischen Infrastrukturen innerhalb des Informationsverbunds ist eindeutig zu kennzeichnen. Hierbei sind alle relevanten Schnittstellen einzubeziehen. Alle einschlägigen Anforderungen der ZAIT 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 bspw. erfolgen, indem im Inventar entsprechend 3.3 ZAIT (bspw. in einer Configuration Management Database CMDB) die Komponenten und Bereiche des Informationsverbunds 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 ZAIT-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. U.a. 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 bspw. 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 Kapitel 9 ZAIT zu berücksichtigen. • Im Rahmen der Notfallvorsorge sind Maßnahmen zu ergreifen (Kapitel 10 ZAIT), mit denen die kritischen Dienstleistungen auch im Notfall aufrechterhalten werden können.
12.5.	Die Nachweiserbringung gemäß § 8a Abs. 3 BSIG bezüglich 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 2020 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.