BaFin

Rundschreiben 10/2017 (BA) vom 03.11.2017

An alle Kreditinstitute
und Finanzdienstleistungsinstitute
in der Bundesrepublik Deutschland

Bankaufsichtliche Anforderungen an die IT (BAIT)

Inhalt

I. Vorbemerkung 3
II. Anforderungen 4
1. IT-Strategie 4
2. IT-Governance 5
3. Informationsrisikomanagement 6
4. Informationssicherheitsmanagement 8
5. Benutzerberechtigungsmanagement 11
6. IT-Projekte, Anwendungsentwicklung (inkl. durch Endbenutzer in den Fachbereichen) 13
7. IT-Betrieb (inkl. Datensicherung) 16
8. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen 19

I. Vorbemerkung

1 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 und für das IT-Risikomanagement - vor. Es präzisiert ferner die Anforderungen des § 25b KWG (Auslagerung von Aktivitäten und Prozessen). 2 Die in den Mindestanforderungen an das Risikomanagement (MaRisk) enthaltenen Anforderungen bleiben 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 auch insbesondere 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 die IT-Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik und der internationale Sicherheitsstandard ISO/IEC 2700X der International Organization for Standardization. 3 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). 4 Der Anwenderkreis dieses Rundschreibens ergibt sich aus AT 2.1 MaRisk entsprechend.	

II. Anforderungen

1. IT-Strategie

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.	
2	Die Geschäftsleitung hat eine mit der Geschäftsstrategie konsistente IT-Strategie festzulegen. Mindestinhalte der IT-Strategie sind: a) Strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation des Instituts sowie der Auslagerungen von IT-Dienstleistungen b) Zuordnung der gängigen Standards, an denen sich das Institut orientiert, auf die Bereiche der IT c) Zuständigkeiten und Einbindung der Informationssicherheit in die Organisation d) Strategische Entwicklung der IT-Architektur e) Aussagen zum Notfallmanagement unter Berücksichtigung der IT-Belange f) Aussagen zu den in den Fachbereichen selbst betriebenen 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. 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 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 Zu d): Darstellung des Zielbilds der IT-Architektur in Form eines Überblicks über die Anwendungslandschaft

2. IT-Governance

3	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).	
4	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 die Regelungen zur IT-Aufbau- und IT-Ablauforganisation wirksam umgesetzt werden.	
5	Das Institut hat insbesondere das Informationsrisikomanagement, das Informationssicherheitsmanagement, den IT-Betrieb und die Anwendungsentwicklung quantitativ und qualitativ angemessen mit Personal auszustatten.	Hinsichtlich der Maßnahmen zur Erhaltung einer angemessenen qualitativen Personalausstattung werden insbesondere der Stand der Technik sowie die aktuelle und zukünftige Entwicklung der Bedrohungslage berücksichtigt.
6	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.
7	Zur Steuerung der für den Betrieb und die Weiterentwicklung der IT-Systeme zuständigen Bereiche durch die Geschäftsleitung sind angemessene quantitative oder qualitative Kriterien festzulegen, und deren Einhaltung ist zu überwachen.	Bei der Festlegung der Kriterien können z. B. die Qualität der Leistungserbringungen, die Verfügbarkeit, Wartbarkeit, Anpassbarkeit an neue Anforderungen, Sicherheit der IT-Systeme oder der dazugehörigen IT-Prozesse sowie deren Kosten berücksichtigt werden.

3. Informationsrisikomanagement

8	Die Informationsverarbeitung und -weitergabe in Geschäfts- und Serviceprozessen wird durch datenverarbeitende IT-Systeme und zugehörige IT-Prozesse unterstützt. Deren Umfang und Qualität ist insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie an der Risikosituation zu orientieren (vgl. AT 7.2 Tz. 1 MaRisk). IT-Systeme und zugehörige IT-Prozesse 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).	
9	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 sind.
10	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, Geschäftsprozesse, IT-Systeme sowie Netz- und Gebäudeinfrastrukturen.
11	Die Methodik zur Ermittlung des Schutzbedarfs (insbesondere im Hinblick auf die Schutzziele „Integrität", „Verfügbarkeit", „Vertraulichkeit" und „Authentizität") hat die Konsistenz der resultierenden Schutzbedarfe nachvollziehbar sicherzustellen.	Schutzbedarfskategorien sind beispielhaft „Niedrig", „Mittel", „Hoch" und „Sehr hoch".
12	Die Anforderungen des Instituts zur Umsetzung der Schutzziele in den Schutzbedarfskategorien sind festzulegen und in geeigneter Form zu dokumentieren (Sollmaßnahmenkatalog).	Der Sollmaßnahmenkatalog enthält lediglich die Anforderung, nicht jedoch deren konkrete Umsetzung.

13 Die Risikoanalyse auf Basis der festgelegten Risikokriterien hat auf Grundlage eines Vergleichs der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen zu erfolgen. Sonstige risikoreduzierende Maßnahmen aufgrund unvollständig umgesetzter Sollmaßnahmen sind wirksam zu koordinieren, zu dokumentieren, zu überwachen und zu steuern. Die Ergebnisse der Risikoanalyse sind zu genehmigen und in den Prozess des Managements der operationellen Risiken zu überführen.	Risikokriterien enthalten bspw. mögliche Bedrohungen, das Schadenspotenzial, die Schadenshäufigkeit sowie den Risikoappetit.
14 Die Geschäftsleitung ist regelmäßig, mindestens jedoch vierteljährlich, insbesondere über die Ergebnisse der Risikoanalyse sowie Veränderungen an der Risikosituation zu unterrichten.	

4. Informationssicherheitsmanagement

15 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.	
16 Die Geschäftsleitung hat eine Informationssicherheitsleitlinie zu beschließen und innerhalb des Instituts angemessen zu kommunizieren. Die Informationssicherheitsleitlinie hat im Einklang mit den Strategien des Instituts zu stehen.	In der Informationssicherheitsleitlinie werden die Ziele und der Geltungsbereich für die Informationssicherheit festgelegt und die wesentlichen organisatorischen Aspekte des Informationssicherheitsmanagements beschrieben. Regelmäßige Überprüfungen und Anpassungen an geänderte Bedingungen werden risikoorientiert vorgenommen. Veränderungen der Aufbau- und Ablauforganisation sowie der IT-Systeme einer Institution (Geschäftsprozesse, Fachaufgaben, organisatorische Gliederung) werden hierbei ebenso berücksichtigt wie Veränderungen der äußeren Rahmenbedingungen (z. B. gesetzliche Regelungen, regulatorische Anforderungen), der Bedrohungsszenarien oder der Sicherheitstechnologien.
17 Auf Basis der Informationssicherheitsleitlinie sind konkretisierende, den Stand der Technik berücksichtigende Informationssicherheitsrichtlinien und Informationssicherheitsprozesse mit den Teilprozessen Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung zu definieren.	Informationssicherheitsrichtlinien werden bspw. für die Bereiche Netzwerksicherheit, Kryptografie, Authentisierung und Protokollierung erstellt. Informationssicherheitsprozesse dienen in erster Linie zur Erreichung der vereinbarten Schutzziele. Dazu gehört u. a., Informationssicherheitsvorfällen vorzubeugen und diese zu identifizieren sowie die angemessene Reaktion und Kommunikation im weiteren Verlauf.
18 Das Institut 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 niedergelegten Ziele und Maßnahmen hinsichtlich der Informationssicherheit sowohl intern als auch gegenüber Dritten transparent gemacht und deren Einhaltung 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) • 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 • Beteiligung bei der Erstellung und Fortschreibung des Notfallkonzepts bzgl. der IT-Belange • die Realisierung von Informationssicherheitsmaßnahmen zu initiieren und zu überwachen • Beteiligung bei Projekten mit IT-Relevanz • als Ansprechpartner für Fragen der Informationssicherheit innerhalb des Instituts und für Dritte bereitzustehen • Informationssicherheitsvorfälle zu untersuchen und diesbezüglich an die Geschäftsleitung zu berichten • Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und zu koordinieren.
19 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 und seinen Vertreter • Festlegung der erforderlichen Ressourcenausstattung für die Funktion des Informationssicherheitsbeauftragten • ein der Funktion zugewiesenes Budget für Informationssicherheits-schulungen 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 Informations-sicherheitsbeauftragten über alle bekannt gewordenen IT-sicherheitsrelevanten Sachverhalte, die das Institut betreffen • Die Funktion des Informationssicherheitsbeauftragten wird aufbauorganisatorisch 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.

20 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 Prozessen 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.
21 Nach einem Informationssicherheitsvorfall sind die Auswirkungen auf die Informationssicherheit zu analysieren und angemessene Nachsorgemaßnahmen zu veranlassen.	Die Definition des Begriffes „Informationssicherheitsvorfall" nach Art und Umfang basiert auf dem Schutzbedarf der betroffenen Geschäftsprozesse, IT-Systeme und den zugehörigen IT-Prozessen. Ein Informations-sicherheitsvorfall kann auch dann vorliegen, wenn mindestens eines der Schutzziele („Verfügbarkeit", „Integrität", „Vertraulichkeit", „Authentizität") gemäß den Vorgaben des institutsspezifischen Sollkonzepts der Informationssicherheit - über dem definierten Schwellenwert - verletzt ist. Der Begriff „Informationssicherheitsvorfall" ist nachvollziehbar vom Begriff „Abweichung vom Regelbetrieb" (im Sinne von „Störung im Tagesbetrieb") abzugrenzen.
22 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 Penetrationstest-Ergebnisse.

5. Benutzerberechtigungsmanagement

23	Ein Benutzerberechtigungsmanagement stellt sicher, dass den Benutzern eingeräumte Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben des Instituts entspricht. Das Benutzerberechtigungsmanagement hat die Anforderungen nach AT 4.3.1 Tz. 2, AT 7.2 Tz. 2, sowie BTO Tz. 9 der MaRisk zu erfüllen.	
24	Berechtigungskonzepte legen den Umfang und die Nutzungsbedingungen der Berechtigungen für die IT-Systeme konsistent zum ermittelten Schutzbedarf sowie vollständig und nachvollziehbar ableitbar für alle von einem IT-System bereitgestellten Berechtigungen fest. Berechtigungskonzepte haben die Vergabe von Berechtigungen an Benutzer nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) sicherzustellen, die Funktionstrennung zu wahren und Interessenskonflikte des Personals zu vermeiden.	Eine mögliche Nutzungsbedingung ist die Befristung der eingeräumten Berechtigungen. Berechtigungen können sowohl für personalisierte, für nicht personalisierte als auch für technische Benutzer vorliegen.
25	Nicht personalisierte Berechtigungen müssen jederzeit zweifelsfrei einer handelnden Person (möglichst automatisiert) zuzuordnen sein. Abweichungen in begründeten Ausnahmefällen und die hieraus resultierenden Risiken sind zu genehmigen und zu dokumentieren.	
26	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 die Umsetzung des Berechtigungsantrags im Zielsystem.
27	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 mit einzubeziehen.	Fällt im Rahmen der Rezertifizierung auf, dass außerhalb des vorgeschriebenen Verfahrens Berechtigungen eingeräumt wurden, so werden diese gemäß der Regelverfahren zur Einrichtung, Änderung und Löschung von Berechtigungen entzogen.

28 Die Einrichtung, Änderung, Deaktivierung sowie Löschung von Berechtigungen und die Rezertifizierung sind nachvollziehbar und auswertbar zu dokumentieren.	
29 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.	Die übergeordnete Verantwortung für die Prozesse zur Protokollierung und Überwachung von Berechtigungen wird einer Stelle zugeordnet, die unabhängig vom berechtigten Benutzer oder dessen Organisationseinheit ist. Aufgrund weitreichender Eingriffsmöglichkeiten privilegierter Benutzer wird das Institut insbesondere für deren Aktivitäten angemessene Prozesse zur Protokollierung und Überwachung einrichten.
30 Durch begleitende technisch-organisatorische Maßnahmen ist einer Umgehung der Vorgaben der Berechtigungskonzepte vorzubeugen.	Technisch-organisatorische Maßnahmen hierzu sind beispielsweise: • Auswahl angemessener Authentifizierungsverfahren • Implementierung einer Richtlinie zur Wahl sicherer Passwörter • automatischer passwortgesicherter Bildschirmschoner • Verschlüsselung von Daten • eine manipulationssichere Implementierung der Protokollierung • Maßnahmen zur Sensibilisierung der Mitarbeiter.

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

31 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.	
32 Die organisatorischen Grundlagen von IT-Projekten (inkl. Qualitätssicherungsmaßnahmen) und die Kriterien für deren Anwendung sind zu regeln.	
33 IT-Projekte sind angemessen zu steuern, insbesondere unter Berücksichtigung der Risiken im Hinblick auf die Dauer, den Ressourcenverbrauch und die Qualität von IT-Projekten. Hierfür sind Vorgehensmodelle festzulegen, deren Einhaltung zu überwachen ist.	Beispielsweise kann die Entscheidung über den Übergang zwischen den Projektphasen von eindeutigen Qualitätskriterien des jeweiligen Vorgehensmodells abhängen.
34 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.
35 Wesentliche IT-Projekte und IT-Projektrisiken sind der Geschäftsleitung regelmäßig und anlassbezogen zu berichten. Wesentliche Projektrisiken sind im Risikomanagement zu berücksichtigen.	
36 Für die Anwendungsentwicklung sind angemessene Prozesse festzulegen, die Vorgaben zur Anforderungsermittlung, zum Entwicklungsziel, zur (technischen) Umsetzung (einschließlich Programmierrichtlinien), zur Qualitätssicherung, sowie zu Test, Abnahme und Freigabe enthalten.	Anwendungsentwicklung umfasst beispielsweise die Entwicklung von Software zur Unterstützung bankfachlicher Prozesse oder die von Endbenutzern in den Fachbereichen selbst entwickelten Anwendungen (z. B. Individuelle Datenverarbeitung – IDV). Die Ausgestaltung der Prozesse erfolgt risikoorientiert.

37 Anforderungen an die Funktionalität der Anwendung müssen ebenso erhoben, bewertet und dokumentiert werden wie nichtfunktionale Anforderungen. Die Verantwortung für die Erhebung und Bewertung der Anforderungen liegt in den Fachbereichen.	Anforderungsdokumente sind beispielsweise: • Fachkonzept (Lastenheft bzw. User-Story) • Technisches Fachkonzept (Pflichtenheft bzw. Product Back-Log). Nichtfunktionale Anforderungen an IT-Systeme sind beispielsweise: • Ergebnisse der Schutzbedarfsfeststellung • Zugriffsregelungen • Ergonomie • Wartbarkeit • Antwortzeiten • Resilienz.
38 Im Rahmen der Anwendungsentwicklung sind nach Maßgabe des Schutzbedarfs angemessene Vorkehrungen im Hinblick darauf zu treffen, dass nach Produktivsetzung der Anwendung die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten nachvollziehbar sichergestellt werden.	Geeignete Vorkehrungen können sein: • Prüfung der Eingabedaten • Systemzugangskontrolle • Nutzer-Authentifizierung • Transaktionsautorisierung • Protokollierung der Systemaktivität • Prüfpfade (Audit Logs) • Verfolgung von sicherheitsrelevanten Ereignissen • Behandlung von Ausnahmen.
39 Im Rahmen der Anwendungsentwicklung müssen Vorkehrungen getroffen werden, die erkennen lassen, ob eine Anwendung versehentlich geändert oder absichtlich manipuliert wurde.	Eine geeignete Vorkehrung unter Berücksichtigung des Schutzbedarfs kann die Überprüfung des Quellcodes im Rahmen der Anwendungsentwicklung sein. Die Überprüfung des Quellcodes ist eine methodische Untersuchung zur Identifizierung von Risiken.
40 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.

41 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 Sicherheitskontrollen und die Systemleistung unter verschiedenen Stressbelastungsszenarien einzubeziehen. Die Durchführung von fachlichen Abnahmetests verantwortet der für die Anwendung zuständige Fachbereich. Testumgebungen zur Durchführung der Abnahmetests haben in für den Test wesentlichen Aspekten der Produktionsumgebung zu entsprechen. Testaktivitäten und Testergebnisse sind zu dokumentieren.	Dies umfasst einschlägige Expertise sowie eine angemessen ausgestaltete Unabhängigkeit von den Anwendungsentwicklern. Eine Testdokumentation enthält mindestens folgende Punkte: • Testfallbeschreibung • Dokumentation der zugrunde gelegten Parametrisierung des Testfalls • Testdaten • erwartetes Testergebnis • erzieltes Testergebnis • aus den Tests abgeleiteten Maßnahmen.
42 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 der Abweichungen vom Regelbetrieb sein.
43 Ein angemessenes Verfahren für die Klassifizierung / Kategorisierung (Schutzbedarfsklasse) und den Umgang mit den von Endbenutzern des Fachbereichs entwickelten oder betriebenen Anwendungen ist festzulegen.	Die Einhaltung von Programmierstandards wird auch für die von Endbenutzern in den Fachbereichen entwickelten Anwendungen (z. B. IDV-Anwendung) sichergestellt. Jede dieser Anwendungen wird einer Schutzbedarfsklasse zugeordnet. Übersteigt der ermittelte Schutzbedarf die technische Schutzmöglichkeit dieser Anwendungen, werden Schutzmaßnahmen in Abhängigkeit der Ergebnisse der Schutzbedarfsklassifizierung ergriffen.
44 Die Vorgaben zur Identifizierung aller von Endbenutzern 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 dieser 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.

7. IT-Betrieb (inkl. Datensicherung)

45 Der IT-Betrieb hat die Erfüllung der Anforderungen, die sich aus der Umsetzung der Geschäftsstrategie sowie aus den IT-unterstützten Geschäftsprozessen ergeben, umzusetzen (vgl. AT 7.2 Tz. 1 und Tz. 2 MaRisk).	
46 Die Komponenten der IT-Systeme sowie 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 • Standort der Komponenten der IT-Systeme • Aufstellung der relevanten Angaben zu Gewährleistungen und sonstigen Supportverträgen (ggf. Verlinkung) • Angaben zum Ablaufdatum des Supportzeitraums der Komponenten der IT-Systeme • Akzeptierter Zeitraum der Nichtverfügbarkeit der IT-Systeme sowie der maximal tolerierbare Datenverlust.
47 Das Portfolio aus IT-Systemen ist angemessen zu steuern. Hierbei werden auch die Risiken aus veralteten IT-Systemen berücksichtigt (Lebens-Zyklus Management).	
48 Die Prozesse zur Änderung von IT-Systemen sind abhängig von Art, Umfang, Komplexität und Risikogehalt auszugestalten und umzusetzen. Dies gilt ebenso für Neu- bzw. Ersatzbeschaffungen von IT-Systemen sowie für sicherheitsrelevante Nachbesserungen (Sicherheitspatches).	Beispiele für Änderungen sind: • Funktionserweiterungen oder Fehlerbehebungen von Software-Komponenten • Datenmigrationen • Änderungen an Konfigurationseinstellungen von IT-Systemen • Austausch von Hardware-Komponenten (Server, Router etc.) • Einsatz neuer Hardware-Komponenten • Umzug der IT-Systeme zu einem anderen Standort.

49 Anträge zur Änderung 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.	Der sicheren Umsetzung der Änderungen in den produktiven Betrieb dienen beispielsweise: • Risikoanalyse in Bezug auf die bestehenden IT-Systeme (insbesondere auch das Netzwerk und die vor- und nachgelagerten IT-Systeme), auch im Hinblick auf mögliche Sicherheits- oder Kompatibilitätsprobleme, als Bestandteil der Änderungsanforderung • Tests von Änderungen vor Produktivsetzung auf mögliche Inkompatibilitäten der Änderungen sowie mögliche sicherheitskritische Aspekte bei maßgeblichen bestehenden IT-Systemen • Tests von Patches vor Produktivsetzung unter Berücksichtigung ihrer Kritikalität (z. B. bei Sicherheits- oder Notfallpatches) • 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).
50 Die Meldungen über ungeplante Abweichungen vom Regelbetrieb (Störungen) und deren Ursachen sind in geeigneter Weise zu erfassen, zu bewerten, insbesondere hinsichtlich möglicherweise resultierender Risiken zu priorisieren und entsprechend festgelegter Kriterien zu eskalieren. Bearbeitung, Ursachenanalyse und Lösungsfindung inkl. Nachverfolgung sind zu dokumentieren. Ein geordneter Prozess zur Analyse möglicher Korrelationen von Störungen und deren Ursachen muss vorhanden sein. Der Bearbeitungsstand offener Meldungen über Störungen, wie auch die Angemessenheit der Bewertung und Priorisierung, ist zu überwachen und zu steuern. Das Institut hat geeignete Kriterien für die Information der Geschäftsleitung über Störungen festzulegen.	Die Identifikation der Risiken kann beispielsweise anhand des Aufzeigens der Verletzung der Schutzziele erfolgen. Die Ursachenanalyse erfolgt auch dann, wenn mehrere IT-Systeme zur Störungs- und Ursachenerfassung sowie –bearbeitung eingesetzt werden.

51 Die Vorgaben für die Verfahren zur Datensicherung (ohne Datenarchivierung) sind schriftlich in einem Datensicherungskonzept zu regeln. Die im Datensicherungskonzept dargestellten Anforderungen an die Verfügbarkeit, Lesbarkeit und Aktualität der Kunden- und Geschäftsdaten sowie an die für deren Verarbeitung notwendigen IT-Systeme sind aus den Anforderungen der Geschäftsprozesse und den Geschäftsfortführungsplänen abzuleiten. Die Verfahren zur Wiederherstellbarkeit im erforderlichen Zeitraum und zur Lesbarkeit von Datensicherungen sind regelmäßig, mindestens jährlich, im Rahmen einer Stichprobe sowie anlassbezogen zu testen.	Die Anforderungen an die Ausgestaltung und Lagerung der Datensicherungen sowie an die durchzuführenden Tests ergeben sich aus diesbezüglichen Risikoanalysen. Hinsichtlich der Standorte für die Lagerung der Datensicherungen können eine oder mehrere weitere Lokationen erforderlich sein.

8. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

52 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).

53 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.
54 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.

55 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 und zum Notfallmanagement, 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 zu berücksichtigen.
56 Die Risikobewertungen in Bezug auf den sonstigen Fremdbezug von IT-Dienstleistungen sind regelmäßig und anlassbezogen zu überprüfen und ggf. inkl. der Vertragsinhalte anzupassen.	