FMA

Dokumentennummer: 01 / 2018
Veröffentlichungsdatum: 08.05.2018

FMA-LEITFADEN

IKT-Sicherheit in Kreditinstituten

STAND Mai 2018

Inhaltsverzeichnis

ZIELSETZUNG UND HINWEISE

Die zunehmende Digitalisierung birgt – neben vielen Vorteilen im Wirtschaftsleben – neue Gefahren und Risiken, denen Unternehmen ausgesetzt sind. Insbesondere die jüngsten Angriffe auf IKT-Systeme von Unternehmen haben deutlich gemacht, wie verwundbar IKT-Infrastrukturen sind. Vor allem für Kreditinstitute, welche immer mehr auf Digitalisierung setzen (müssen), hat sich die Risikolage dadurch deutlich verschärft.

Die Finanzmarktaufsichtsbehörde (FMA) ist sich der immer bedeutender werdenden Möglichkeiten und Risiken, welche aus der Informations- und Kommunikationstechnologie (IKT) resultieren, bewusst und sieht sich aufgrund der gestiegenen Risikolage einer intensivierten IKT-Aufsicht verpflichtet. Aus diesem Grund wird den Instituten seitens der FMA ein Überblick über Ausgestaltung, Anforderungen und Vorkehrungen betreffend die IKT-Sicherheit von Kreditinstituten als Orientierungshilfe zur Verfügung gestellt.

Dieser Leitfaden stellt keine Verordnung dar. Er soll für die beaufsichtigten Institute Know-how aufbereiten und die Entwicklung eines gemeinsamen Verständnisses fördern. Über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten können aus diesem Leitfaden nicht abgeleitet werden.

Dieser Leitfaden richtet sich primär an Kreditinstitute im Sinne des § 1 Abs. 1 BWG, kann jedoch auch von Zahlungsinstituten, E-Geldinstituten und Sonderkreditinstituten[1] zur Orientierung herangezogen werden.[2]

Die Ausführungen in diesem Leitfaden sind unter dem Grundsatz der Proportionalität zu sehen, sodass die Art, der Umfang und die Komplexität der Geschäfte sowie die Risikostruktur des jeweiligen Instituts, in der tatsächlichen Umsetzung der nachfolgenden Ausführungen Berücksichtigung zu finden haben. Anhand dieser Kriterien hat das jeweilige Kreditinstitut zu bestimmen, welche Methoden, Systeme und Prozesse in Bezug auf die IKT-Sicherheit, aufgrund der angebotenen Dienstleistungen, angemessen sind.

[1] Hinzuweisen ist, dass für Kapitalanlagegesellschaften, Immobilienkapitalanlagegesellschaften und Betriebliche Vorsorgekassen ein gesonderter FMA-Leitfaden geplant ist.
[2] Im Falle von IKT-Auslagerungen können sich auch Dienstleister an diesem Leitfaden orientieren.

1. RECHTSGRUNDLAGEN UND GRUNDLEGENDES

Ziel dieses Leitfadens ist es, auf der Grundlage von § 39 Abs. 2b Z 5 und Abs. 4 BWG iVm § 11 KI-RMV (operationelles Risiko), einen Überblick über Ausgestaltung und Vorkehrungen betreffend die IKT-Sicherheit der Kreditinstitute zu geben. Der Inhalt des Leitfadens ist nicht abschließender Natur. Die rechtlichen Grundlagen bleiben durch diesen Leitfaden unberührt.

Für ein einheitliches Begriffsverständnis werden nachstehend die maßgeblichen Definitionen in Bezug auf IKT-Sicherheit dargestellt:

- **Informations- und Kommunikationstechnologie (IKT)**
  umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören die Erhebung, die Erfassung, die Nutzung, die Speicherung, die Übermittlung, die programmgesteuerte Verarbeitung, die interne Darstellung und die Ausgabe von Informationen.

- **IKT-Risiko[3]**
  ist das bestehende oder künftige Risiko von Verlusten aufgrund der Unzweckmäßigkeit oder des Versagens der Hard- und Software technischer Infrastrukturen, welche die Verfügbarkeit, Integrität, Zugänglichkeit und Sicherheit dieser Infrastrukturen oder von Daten beeinträchtigen können. Darunter kann das Risiko aus IKT-Verfügbarkeit und -Kontinuität, IKT-Sicherheit, IKT-Änderungen, IKT-Datenintegrität und IKT-Auslagerungen fallen.

Im Zuge der Umsetzung dieser Orientierungshilfe durch die Institute sollten potentielle Interessenkonflikte und unvereinbare Tätigkeiten bspw. in Doppelfunktionen vermieden werden.

Die Verantwortung für eine angemessene Begrenzung des IKT-Risikos obliegt den Geschäftsleitern. Sie initiieren, steuern, hinterfragen und kontrollieren diesbezügliche Strategien und Verfahren und stellen die Kohärenz mit den strategischen Zielen sicher.

Der vorliegende Leitfaden basiert insbesondere auf den relevanten Bestimmungen der EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process

[3] Festzuhalten ist, dass unter „IT-Risiko“, „IKT-Risiko“ bzw. „Informationssystemrisiko“ das gleiche Risiko adressiert wird und es sich um synonyme Begriffe handelt. In Orientierung an den EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) (EBA/GL/2014/13) und den EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) (EBA/GL/2017/05) wird in diesem Leitfaden der IKT-Begriff verwendet.

(SREP) (EBA/GL/2017/05)[4], dem Basel Committee on Banking Supervision's standard number 239[5] und den CEBS Guidelines on Outsourcing[6].

Bei der Umsetzung zur Behandlung von IKT-Risiken empfiehlt es sich, auf etwaige etablierte Standards zurückzugreifen. Dazu gehören unter anderem:

- **ITIL**[7]
  Die IT Infrastructure Library (ITIL) ist ein etablierter Qualitätsstandard, indem sich vordefinierte Prozesse, Funktionen und Rollen für IKT-Infrastrukturen von Unternehmen finden (Sammlung von Best Practices für Service Management).

- **BSI-Grundschutz**[8]
  Der BSI-Grundschutz ist eine Sammlung von Dokumenten des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI), die zur Erkennung und Bekämpfung sicherheitsrelevanter Schwachstellen in IKT-Umgebungen dienen.

- **COBIT**[9]
  Das Rahmenwerk Control Objectives for Information and related Technology (COBIT) ermöglicht die Steuerung und Kontrolle des IKT-Betriebs durch das Management. COBIT entstand aus einer Sammlung von mehreren IKT-Standards, Rahmenwerken, Richtlinien und Best Practices.

- **ISO 27001**[10]
  Die ISO 27001 wurde erarbeitet für die Einrichtung, Implementierung, Wartung und laufende Verbesserung eines Informationssicherheitsmanagementsystems.

- **Österreichisches Informationssicherheitshandbuch**[11]
  Dieses beschreibt und unterstützt die Vorgehensweise zur Etablierung eines umfassenden Informationssicherheitsmanagementsystems in Unternehmen und der öffentlichen Verwaltung. Das Handbuch eignet sich beispielsweise als Implementierungshilfe für die Umsetzung für die ISO 27001.

[4] https://www.eba.europa.eu/documents/10180/1954038/Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29_DE.pdf/
[5] https://www.bis.org/publ/bcbs239.pdf
[6] https://www.eba.europa.eu/documents/10180/104404/GL02OutsourcingGuidelines.pdf.pdf
[7] https://www.axelos.com/best-practice-solutions/itil
[8] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
[9] http://www.isaca.org/cobit/pages/default.aspx
[10] https://www.iso.org/standard/54534.html
[11] https://www.sicherheitshandbuch.gv.at/

2. IKT-STRATEGIE

Geschäftsleiter[12] von Instituten sind für die Erstellung einer mit der Geschäftsstrategie übereinstimmenden IKT-Strategie, welche im Einklang mit Art, Umfang und Komplexität der IKT-Tätigkeiten steht, verantwortlich.

Die IKT-Strategie steht im Einklang mit der allgemeinen Geschäftsstrategie und unterstützt das Geschäftsmodell. Dabei beinhaltet die IKT-Strategie die strategischen Leitlinien zur IKT. Ausführungen zur operativen Umsetzung sind in nachgeordneten Regelwerken enthalten.

Die IKT-Strategie unterliegt der Genehmigung und Aufsicht durch die Geschäftsführung und wird in regelmäßigen Abständen sowie anlassbezogen auf ihre Aktualität überprüft und gegebenenfalls (orientiert an den Geschäftszielen) angepasst.

Mit Hilfe der IKT-Strategie und den darauf aufbauenden Awarenessmaßnahmen wird ein unternehmens- und gruppenweites Bewusstsein für Informationssicherheit geschaffen. Dies erfolgt bspw. durch: Kommunikation auf Gruppenebene, entsprechende Trainings, Maßnahmen zur Bewusstseinsbildung der Mitarbeiter.

Zu beachten ist dabei, dass die IKT-Strategie eine wichtige Informationsquelle für die IKT-Revision und für die Einbindung der IKT in die Ertrags- und Risikosteuerung ist. Die Innenrevision ist als unabhängige Kontrollfunktion eingebunden um sicherzustellen, dass die mit der Umsetzung der IKT-Strategie verbundenen Risiken bewertet und wirksam gemindert werden. Daher enthält die IKT-Strategie auch Aussagen zur geplanten Ausgestaltung der IKT, wodurch Planungssicherheit für die IKT-Organisation, taktische IKT-Planung und Ressourcenplanung ermöglicht wird.

Ziel ist es, einen proaktiven Austausch zwischen der IKT-Organisation und den Entscheidungsträgern zu schaffen, eine klare Kompetenzordnung zu erstellen und gegebenenfalls Ausschüsse für IKT- und Fachbereiche einzurichten. Dabei wird sichergestellt, dass die Geschäftsleitung alle entscheidungsrelevanten Informationen rechtzeitig und im nötigen Umfang erreichen.

In der IKT-Strategie werden die strategische Entwicklung, der IKT-Aufbau- und Ablauforganisation inklusive der dazugehörigen Prozesse, festgelegt. Hierbei orientieren sich die Institute an bestehenden Standards (z.B. ISO 27001, BSI-Grundschutz).

[12] Die Begriffe „Geschäftsleiter“, „Geschäftsführung“ und „Unternehmensführung“ werden im gegenständlichen Leitfaden synonym verwendet. Sollten im Folgenden ausnahmsweise unterschiedliche Aspekte angesprochen werden, wird darauf gesondert hingewiesen.

Des Weiteren nehmen Institute unter anderem folgende Punkte in die IKT-Strategie auf:

- Entwicklung einer IKT-Zielarchitektur mit einem Überblick über die Anwendungslandschaft,
- Festlegung von Zuständigkeiten, Rollen und Aufgaben für einen systemischen Informationssicherheitsprozess,
- Berücksichtigung von Auslagerungsaspekten,
- Festlegung eines Notfallmanagements und
- Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IKT-Systemen (Hardware und Software).

Wesentliche dabei zu berücksichtigende sicherheitsrelevante Themen sind bspw. die Sicherheitsrisiken für das Institut und deren Informationen sowie die damit verbundenen Auswirkungen und Kosten, Auswirkungen von Sicherheitsvorfällen auf die kritischen Geschäftsprozesse, Sicherheitsanforderungen aus gesetzlichen und vertraglichen Vorgaben, branchentypische Standardvorgehensweisen zur Informationssicherheit, der Stand der Informationssicherheit und daraus abgeleitete Handlungsempfehlungen.

Schließlich achten die Institute darauf, dass der Sicherheitsprozess von allen Mitarbeitern mitgetragen wird.

3. IKT-GOVERNANCE

Die IKT-Governance baut auf der IKT-Strategie des Instituts auf und ist ein wesentlicher Bestandteil der Unternehmensführung. Sie liegt in der Verantwortung der Geschäftsleitung und stellt sicher, dass die IKT die Unternehmensziele und -strategie optimal unterstützt. Die IKT-Governance setzt sich u.a. aus folgenden wesentlichen Elementen zusammen: Prozessstrukturen, Organisationsvorgaben und Führungsstrukturen für die komplette IKT-Infrastruktur im Institut. Zweck der IKT-Governance ist somit die Steuerung und Überwachung des Betriebs und der Weiterentwicklung der im Institut verwendeten IKT-Systeme samt der dazugehörigen IKT-Prozesse.

Es liegt im Verantwortungsbereich der Geschäftsleitung – im Einklang mit der IKT-Strategie – Regelungen zur Umsetzung der IKT-Aufbau- und IKT-Ablauforganisation festzulegen (z.B. IKT-Risikomanagementrichtlinien, etc.). Dabei gilt es insbesondere, unvereinbare Tätigkeiten und Interessenkonflikte (z.B. Trennung von anwendungsentwickelnden Tätigkeiten und Tätigkeiten im Zuge des Testbetriebs) zu vermeiden. Zudem werden Prozesse bei Änderungen der Risikosituation oder Rahmenbedingungen zeitnah angepasst.

Die Geschäftsleitung stattet das IKT-Risikomanagement (insb. Informationsrisiko-management, Informationssicherheitsmanagement, IKT-Betrieb und Anwendungs-entwicklung) entsprechend der Art, dem Umfang, der Komplexität der betriebenen Bankgeschäfte und unter Berücksichtigung der aktuellen und zukünftigen Risikosituation

quantitativ und qualitativ angemessen mit Ressourcen/Personal aus. Die Geschäftsleitung stellt sicher, dass ein in Bezug auf Aufbau und Ausführung angemessenes Internes Kontrollsystem (IKS) gemäß § 39 Abs. 2 Z 5 und Abs. 4 BWG in Verbindung mit § 11 KI-RMV eingerichtet und dokumentiert ist.

Institute verfügen über Prozesse zur Identifikation, Bewertung, Steuerung und Überwachung der wesentlichen IKT-Risiken und evaluieren diese laufend. Ebenso verfügt das Institut über eine klare Abgrenzung der Rollen bzw. Verantwortlichkeiten betreffend Identifikation, Beurteilung, Monitoring, Minimierung, Reporting und Beaufsichtigung der wesentlichen IKT-Risiken. Insbesondere ist darauf zu achten, dass diese Themen entsprechend § 42 BWG im Zuge von Prüfungen durch die Interne Revision berücksichtigt werden bzw. durch Einbeziehung externer Experten auf Effektivität zu überprüfen sind.

Abschließend ist festzuhalten, dass die Unternehmensführung ausreichende Ressourcen für die Behandlung von IKT-Risiken zur Verfügung stellt. Des Weiteren sorgen sie auch für eine angemessene Aus- und Weiterbildung der betroffenen Mitarbeiter. Darüber hinaus berücksichtigt die Interne Revision des Instituts im Rahmen der Audit Planung, IKT-Risiken und deren Behandlung in adäquater Weise.

4. SICHERHEITSRICHTLINIEN

Ein wesentliches Instrument zum Schutz von Informationen sind Sicherheitsrichtlinien. Diese beziehen sich nicht nur auf die Sicherheit der IKT-Systeme und der darin gespeicherten Daten, sondern umfassen auch generell das Thema Informationssicherheit (und somit auch die Sicherheit von nicht elektronisch verarbeiteten Informationen). Der Schutz der IKT-Systeme ist nur als Teilaspekt der Informationssicherheit zu sehen.

Das zentrale Dokument auf höchster Ebene ist die Richtlinie zur Informationssicherheit. In dieser wird der Ansatz zur Bewältigung von Informationssicherheitszielen festgelegt. Des Weiteren werden die Ziele und Grundsätze des Instituts im Umgang mit Informationssicherheit beschrieben und der Umfang entsprechend festgelegt. Als Grundlage für den Inhalt dienen die Anforderungen aus der Unternehmensstrategie, Vorschriften, Gesetze und Verträge sowie das aktuelle und zukünftige Umfeld von Bedrohungen in Bezug auf Informationssicherheit.

Die Informationssicherheitsrichtlinie ist Ausgangspunkt für themenspezifische bzw. konkretisierende Richtlinien und Prozesse für Teilbereiche, wie bspw. Netzwerksicherheit, Kryptografie, Authentisierung, Protokollierung, physische Sicherheit/Absicherung der Gebäude und Datacenter, sichere Verwahrung von physischen Daten, etc. Dabei werden Schutzmaßnahmen, Methoden zur Identifikation, Reaktionen und Wiederherstellungsabläufe bei Sicherheitsvorfällen definiert.

Jede Richtlinie wird in planmäßigen Abständen oder nach erheblichen Änderungen auf deren Wirksamkeit und Geeignetheit überprüft. Des Weiteren werden die Richtlinien durch die Unternehmensführung genehmigt. Darüber hinaus sind die Richtlinien sämtlichen betroffenen Personen im Institut bekannt und jederzeit verfügbar.

5. INFORMATIONSRISIKOMANAGEMENT UND -SICHERHEITSMANAGEMENT/CYBER-SICHERHEIT

Als Folge der wachsenden Bedeutung der im Institut eingesetzten IKT-Systeme wird der Ausgestaltung der IKT-Prozesse zum Schutz von Daten und kritischen Informationen bzw. dem gesamten Informationsrisikomanagement stärkere Beachtung geschenkt.

Die nachfolgenden Ausführungen beziehen sich insbesondere auf die IKT-relevanten Aspekte der Informationssicherheit, können aber sinngemäß für die gesamte Informationssicherheit herangezogen werden.

Das Informationsrisikomanagement gewährleistet daher, dass die Informationsverarbeitung und -weitergabe im Institut durch adäquate IKT-Systeme (Hard- und Softwarekomponenten) und Prozesse unterstützt wird. Bei der Ausgestaltung derselben wird beachtet, dass die Integrität, die Verfügbarkeit, die Authentizität und die Vertraulichkeit der Daten gewährleistet ist. Bezüglich deren Umfang und Qualität erfolgt eine Orientierung an den betriebsinternen Erfordernissen, den Geschäftsaktivitäten und der Risikosituation. In diesem Zusammenhang wird eine entsprechende Risikoanalyse und -bewertung durchgeführt, sodass alle relevanten Informationen des Unternehmens entsprechend berücksichtigt werden.

Diese Prozesse werden von der Geschäftsleitung beschlossen und angemessen im Institut und gegebenenfalls an externe Service Provider kommuniziert. Die diesbezüglichen Prozesse stehen im Einklang mit der Strategie des Instituts und berücksichtigen den aktuellen Stand der Technik. Die Prozesse werden regelmäßig evaluiert und risikoorientiert an geänderte Rahmenbedingungen angepasst (z.B. Änderungen in der Aufbau- und Ablauforganisation, der gesetzlichen Rahmenbedingungen, der regulatorischen Anforderungen, der Bedrohungsszenarien, der Sicherheitstechnologie).

Im Zuge der Etablierung eines Informationsrisikomanagementsystems im Institut werden Interessenkonflikte bei der Zuordnung von Personen und Rollen vermieden. Zudem wird die Berücksichtigung von Schnittstellen und Abhängigkeiten von geschäftsrelevanten Informationen, Geschäftsprozessen, IKT-Systemen, Netz- und Gebäudeinfrastrukturen, etc. sichergestellt.

Bezüglich der Risikoüberwachung und -steuerung verfügt das Institut über eine Methodik zur Ermittlung des Schutzbedarfs in Bezug auf Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität von Informationen. Zudem werden die Informationen in unterschiedliche Schutzbedarfskategorien eingeteilt. Im Rahmen des Informationsrisikomanagements werden sämtliche kritische IKT-Systeme und -Services (z.B. Kernprozesse des Instituts, sensible Daten mit hohem Schadenspotential bei Verlust) anhand von festgelegten Kriterien identifiziert. Des Weiteren ist ein präventiver Maßnahmenkatalog zur Reduzierung der festgestellten Risiken vorhanden. Eine angemessene Dokumentation (bspw. tatsächlich umgesetzte Maßnahmen, Risikobeurteilung) wird sichergestellt.

Auf eine laufende Risikoanalyse (z.B. mögliche Bedrohungen, Schadenspotenzial, Schadenshäufigkeit, Risikoappetit, mögliche Reputationsschäden, Nichterfüllung regulatorischer Anforderungen) wird geachtet und wird eine regelmäßige Information der Geschäftsleitung über die Risikosituation bzw. deren Veränderung gewährleistet. Zur Risikoidentifizierung werden unter anderem folgende Faktoren herangezogen:

- Komplexität der IKT-Infrastruktur und der Datenverarbeitungsprozesse,
- Wesentliche Änderungen von IKT-Systemen und Funktionen und
- Abhängigkeiten von ausgelagerten Dienstleistungen und Serviceleistungen Dritter (z.B. Provider, etc.).

Das Institut richtet aufgrund der Art, dem Umfang und der Komplexität der betriebenen Bankgeschäfte und unter Berücksichtigung der aktuellen und zukünftigen Risikosituation die Funktion eines Informationssicherheitsbeauftragten ein, dessen zentrale Aufgabe die Verantwortung aller Belange der Informationssicherheit innerhalb des Instituts und gegenüber Dritten ist. Darüber hinaus ist er auch für die Überprüfung und Überwachung der Einhaltung der Informationssicherheitsprozesse und -richtlinien zuständig. Sofern im Institut etabliert, unterstützt der Informationssicherheitsbeauftragte zudem die Geschäftsleitung bei der Festlegung und Anpassung der Informationssicherheitsrichtlinie, steht dieser beratend zur Seite und berichtet dieser regelmäßig. Darüber hinaus obliegen ihm die Durchführung von Schulungsmaßnahmen und die Setzung von Sensibilisierungsmaßnahmen im Institut betreffend die Informationssicherheit. Weitere Aufgaben sind bspw. die Beteiligung bei der Erstellung von Notfallkonzepten und Projekten mit IKT-Relevanz sowie die Untersuchung von Sicherheitsvorfällen. Zudem steht der Informationssicherheitsbeauftragte mit seiner Expertise betroffenen Abteilungen zur Verfügung.

Die Funktion des Informationssicherheitsbeauftragten ist grundsätzlich organisatorisch und prozessual unabhängig ausgestaltet und im eigenen Institut vor Ort etabliert. Institute können im Rahmen eines Sektorverbundes ohne wesentliche eigenbetriebene IKT auch einen gemeinsamen Informationssicherheitsbeauftragten bestellen, wobei dem Informations-sicherheitsbeauftragten im Institut ohne Informationssicherheitsbeauftragten vor Ort eine zuständige fachkundige bzw. geschulte Ansprechperson zur Verfügung steht.

Das Institut analysiert nach Sicherheitsvorfällen die Auswirkungen auf die Informationssicherheit und veranlasst angemessene Nachsorgemaßnahmen.

Institute adressieren die Cyber-Sicherheit[13] als Teil der IKT-Sicherheit und treten den Bedrohungen aus dem Cyberspace[14] entgegen, indem die reale Betroffenheit, der Schutzbedarf und das anzustrebende Sicherheitsniveau definiert werden. Für eine angemessene Cyber-Sicherheit im Institut kommen unter anderem folgende Maßnahmen in Betracht: Absicherung von Netzübergängen, Abwehr von Schadprogrammen, Vermeidung von offenen Sicherheitslücken, sichere Interaktion mit dem Internet, regelmäßige Logdatenerfassung und -auswertung, Sicherstellung eines aktuellen Informationsstands, Bewältigung von Sicherheitsvorfällen, Durchführung nutzerorientierter Maßnahmen.

Zum Schutz der IKT-Systeme sowie von kritischen und sensiblen Daten vor Cyber-Attacken, werden Verwundbarkeitsanalysen und regelmäßige Penetrationstests (Ausnutzen von Software-Schwachstellen und Sicherheitslücken in der IKT-Infrastruktur, um unberechtigten Zugang zu dieser zu erhalten) durchgeführt. Hierfür ist qualifiziertes Personal mit angemessenen Ressourcen einzusetzen. Die Erkenntnisse dieser Tests fließen in die relevanten Sicherheitsrichtlinien und das IKT-Risikomanagement ein.

Im Falle einer erfolgreich durchgeführten Cyber-Attacke, stellt das Institut den entstandenen Schaden unter Beiziehung eines IKT-Forensikers oder des Informationssicherheitsbeauftragten fest und dokumentiert diesen in einem Schadensbericht. Mithilfe des Schadensberichts werden etwaige Mängel oder Fehlplanungen (bspw. in der Organisation oder im Budget) aufgezeigt, um künftigen Cyber-Attacken vorzubeugen.

6. BENUTZERBERECHTIGUNGSMANAGEMENT

Das Benutzerberechtigungsmanagement umfasst alle Prozesse, die der Autorisierung eines Anwenders (inklusive privilegierter Benutzer) hinsichtlich Berechtigungen auf IKT-Ressourcen (Einrichtung, Zugriff und Nutzung, Bearbeitung, Deaktivierung, Löschung) dienen.

Ziel des Benutzerberechtigungsmanagements ist es, dass nur autorisierte Benutzer im Institut auf IKT-Services und -Anwendungen zugreifen können. Zudem soll vor allem missbräuchliche Verwendung und unautorisierte Manipulation von Daten und IKT-Systemen verhindert werden.

Das Institut verfügt über ein dokumentiertes Berechtigungskonzept und Benutzerberechtigungsprozesse. Die Vergabekriterien von Berechtigungen berücksichtigen

[13] Cyber-Sicherheit verfolgt den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gegen Bedrohungen aus dem Cyberspace.
[14] Unter dem Begriff Cyberspace ist das komplexe Umfeld zu verstehen, welches aus der Interaktion von Menschen, Software und Diensten im Internet durch daran angeschlossene technische Hilfsmittel und Netzwerke entsteht, die in keiner physischen Form existieren.

dabei den Grundsatz der minimalen Rechtevergabe bzw. das Need-to-know-Prinzip und sind nachvollziehbar sowie konsistent. Zudem werden Funktionstrennungen gewahrt und Interessenkonflikte vermieden. Im Rahmen des Berechtigungskonzepts werden unter anderem das Passwortmanagement (Komplexität, Länge und Lebensdauer von Passwörtern) und Richtlinien für Sonderberechtigungen (z.B. Administrationsrechte, Systemaccounts, etc.) berücksichtigt.

Das gemeinsame Verwenden von Zugangsdaten (z.B. bei Webapplikationen, nicht personenbezogenen Adminaccounts, etc.) zu Systemen wird verhindert. Abweichungen in Ausnahmefällen werden genehmigt und dokumentiert.

Die Einräumung, Änderung, Deaktivierung und Löschung von Berechtigungen ist nachvollziehbar, zuordenbar und auswertbar dokumentiert. Die Freigabe der Zugriffsberechtigungen erfolgt durch einen Business Data Owner oder einen Information Owner. Eingeräumte Berechtigungen werden – trotz Kontrollen der operativen Einheit – regelmäßig durch eine unabhängige Stelle (bspw. Interne Revision) dahingehend überprüft, ob sie dem Berechtigungskonzept bzw. den -prozessen entsprechen, nur wie vorgesehen eingesetzt werden und auch weiterhin benötigt werden, wobei auf eine entsprechende Dokumentation geachtet wird. Durch technisch-organisatorische Maßnahmen (z.B. angemessene Authentifizierungsverfahren, Verschlüsselung von Daten, technische Protokollierung von Benutzer- und Administratorentätigkeiten („Logging“) wird eine Manipulation der Berechtigungskonzepte verhindert.

7. SCHWACHSTELLENMANAGEMENT

Schwachstellenmanagement als integraler Bestandteil der IKT-Sicherheit ist ein zyklischer Prozess zur Identifikation, Klassifizierung und Beseitigung von Schwachstellen insbesondere in Software und Firmware.

Institute verfügen über angemessene Verfahren, Prozesse und technisch-organisatorische Maßnahmen, um Daten vor Verlust bzw. Beschädigung zu schützen. Gleiches gilt für den Schutz vor Schadprogrammen („Malware“), Datendiebstahl und Cyberkriminalität.

Institute identifizieren die Schwachstellen in ihren Systemen, ergreifen Maßnahmen zur Schwachstellenbeseitigung und überprüfen regelmäßig die Wirksamkeit der umgesetzten Maßnahmen. Bspw. werden im Rahmen des Schwachstellenmanagements regelmäßige Überprüfungen des Netzwerks und des Firewall-Logging durch Penetrationstests oder Virenscanner durchgeführt.

Weiters analysieren Institute die Auswirkungen der Schwachstellen (auf Server, Anwendungen, Netzwerke oder Systeme) und klassifizieren deren Risiko, um in einem

weiteren Schritt Strategien festlegen zu können, wie Schwachstellen künftig verhindert und besser beseitigt werden können.

Ein Virenschutzprogramm zum Schutz vor Schadsoftware ist heutzutage nicht mehr ausreichend, weshalb zusätzliche Schutzmaßnahmen getroffen werden. Dazu gehören bspw.:

- Zeitnahe Installation von aktuellen Sicherheitsupdates,
- Klare organisatorische und technische Regelungen unter anderem bei der Konfiguration und Administration von Firewalls und
- Regelmäßige Überprüfung der Funktionalität der Datensicherung (Backup und Restore).

Da sich die Risikosituation ständig verändert wird das Schwachstellenmanagement regelmäßig evaluiert.

8. IKT-PROJEKTE, ANWENDUNGSENTWICKLUNG UND ZUGEKAUFTE SOFTWARE[15]

Institute erstellen im Falle von IKT-Projekten eine Analyse, die vorab die damit einhergehenden wesentlichen Veränderungen in den IKT-Systemen – in Hinblick auf deren Auswirkung auf die IKT-Aufbau- und IKT-Ablauforganisation sowie die dazugehörigen IKT-Prozesse – aufzeigt und eine Bewertung der damit verbundenen Risiken vornimmt.

Um mögliche Beeinträchtigungen des Risikoprofils des Instituts identifizieren zu können, werden IKT-Projekte angemessen gesteuert, deren Risiken laufend berücksichtigt und dies vollständig dokumentiert. Institute überwachen und steuern die festgelegten Vorgehensmodelle bei IKT-Projekten und deren Portfolio angemessen. Der Geschäftsleitung werden wesentliche IKT-Projekte und deren Risiken in regelmäßigen Intervallen und anlassbezogen berichtet. Im Rahmen ihrer Aufgaben erfolgt die Einbeziehung von einzelnen Organisationseinheiten des Instituts an den IKT-Projekten (Risikomanagement, Compliance, Interne Revision).

Für Anwendungsentwicklungen (v.a. Eigenentwicklungen) werden angemessene Prozesse festgelegt, welche auch den Fachbereich im erforderlichen Maß einbinden. Die Prozesse enthalten Vorgaben hinsichtlich Anforderungen, Ziele, Umsetzung, Qualitätssicherung, Test, Abnahme und Freigabe der Anwendung. Die Anwendung und deren Entwicklung werden insbesondere in Bezug auf vorgenommene Änderungen angemessen dokumentiert, um etwaigen Manipulationen vorzubeugen (Software-Quellcode-Kontrollsystem). In diesem Zusammenhang wird auf die jederzeitige Vertraulichkeit, Integrität, Verfügbarkeit und

[15] Die nachstehenden Ausführungen sind sinngemäß auch für zugekaufte Software zu berücksichtigen.

Authentizität der zu verarbeitenden Daten – bereits vor der Produktion bis hin zum Austausch, Archivieren, Entsorgen oder Vernichten von Anwendungen – geachtet (Sicherheitslücken-Screening). Zudem implementieren Institute Programmierrichtlinien.

Für die mehrstufigen Anwendungstests vor Produktivsetzung bzw. nach wesentlichen Änderungen wird eine Methodik implementiert, die unter verschiedenen Stressbelastungsszenarien die Funktionalität der Anwendung, die Sicherheitskontrollen und die Systemleistungen abdeckt. In diesem Zusammenhang werden neben der Produktionsumgebung entsprechende Entwicklungs- und Testumgebungen implementiert. Testumgebungen stellen eine Abbildung der Produktionsumgebung dar.[16] Die Produktivsetzung von System- bzw. Anwendungsänderungen erfolgen erst nach ausführlichen Tests, um etwaige Störungen des Geschäftsbetriebs zu verhindern. Neben den funktionalen Tests werden auch sicherheitsrelevante Aspekte (non-functional requirements) getestet. Die Testaktivitäten und -ergebnisse werden dokumentiert. Die zuständige Fachabteilung trägt bei Anwendungsentwicklungen sowohl die Verantwortung für die Erhebung, die Bewertung, die Dokumentation der maßgeblichen Anforderungen, als auch für den Abnahmetest der Anwendung. Nach Produktivsetzung wird der Betrieb laufend überwacht. Bei Abweichungen vom Regelbetrieb werden die entsprechenden Maßnahmen veranlasst. Die Institute verfügen über einen Prozess zur Verwaltung und Überwachung der Lebenszyklen der verwendeten IKT-Systeme (Hard- und Softwarekomponenten), um sicherzustellen, dass diese den aktuellen Anforderungen an das Geschäfts- und Risikomanagement entsprechen und Softwareentwicklungen seitens des Anbieters weiterhin möglich sind.

Im Falle von durch Endbenutzer in den Fachbereichen des Instituts entwickelten und betriebenen Anwendungen wird sowohl eine Richtlinie zur Individuellen Datenverarbeitung (inklusive Regelungen zur Identifizierung solcher Anwendungen, Dokumentation, Testmethodik, Schutzbedarfsklassifizierung, Einhaltung von Programmierstandards, Rezertifizierung der Berechtigungen usw.) als auch ein zentrales Register dieser Anwendungen geführt.

Das Institut verfügt über einen unabhängigen Überprüfungs- und Validierungsprozess, um eine maximal mögliche Reduktion der Risiken bei der Durchführung von Änderungen an IKT-Systemen sicherzustellen. Damit wird erheblich nachteiligen Auswirkungen auf die Verfügbarkeit, Kontinuität und Sicherheit des Instituts vorgebeugt.

Institute verfügen somit über eine umfassende schriftliche Regelung, indem sich sämtliche oben genannten Anforderungen wiederfinden.

[16] In der Praxis werden teilweise in einer Testumgebung Echtdaten verwendet, damit kritische IKT-Umsetzungen lückenlos getestet werden können, z.B. Jahresabschluss. Die Informationen aus der Testumgebung mit Echtdaten darf selbstverständlich nur speziell berechtigten Usern zugänglich sein, um die Sicherheit der Daten entsprechend zu schützen.

9. IKT-BETRIEB UND DATENINTEGRITÄT

Als IKT-Betrieb ist in diesem Zusammenhang die Organisationseinheit eines Unternehmens gemeint, welche die Aufgabe hat, die erforderliche IKT-Infrastruktur (Hard- und Software) in angemessenem Umfang zur Verfügung zu stellen und störungsfrei zu betreiben.[17] Die Anforderungen an den IKT-Betrieb eines Instituts ergeben sich aus der Geschäftsstrategie und lassen sich aus den IKT unterstützten Geschäftsprozessen ableiten. Die Funktionsweise des IKT-Betriebs wird im Rahmen eines Betriebskonzeptes festgehalten.

Institute verwalten die IKT-Komponenten und deren Beziehungen untereinander sowie die dazugehörigen Bestandsangaben, aktualisieren diese regelmäßig und anlassbezogen (Inventarliste) und steuern diese unter Beachtung der Risiken aus dem Lebenszyklus-Management. Weiters bestehen Prozesse zur Neu- bzw. Ersatzbeschaffung sowie Nachbesserung unter Berücksichtigung möglicher Umsetzungsrisiken. Zudem stellen Institute die laufende Wartung ihrer IKT-Systeme sicher und sind entsprechende Wartungsverträge vorhanden.

Für entsprechende Kontrollen wird unter anderem in folgenden Themenbereichen gesorgt:

- Betriebsautomatisierung (z.B. Jobsteuerung),
- Überwachung des laufenden Betriebs,
- Umgang mit veralteter bzw. nicht mehr vom Hersteller unterstützter Software,
- Performance und Kapazitätsmanagement und
- Anforderungen hins. „Secure Operations“.

Störungsmeldungen werden vom Institut in geeigneter Weise erfasst, bewertet und priorisiert. Kriterien hinsichtlich einer Information der Geschäftsleiter sind festgelegt. Ein Prozess zur Vorgehensweise bei Störmeldungen liegt vor, dieser beinhaltet jedenfalls mögliche Korrelationen von Störungen und deren Ursachen, die Vorgehensweise der Bearbeitung, Ursachenanalyse, Lösungsfindung und Nachverfolgung.

Institute verfügen über einen schriftlichen Rahmen für die Ermittlung, das Verständnis, die Messung und die Minderung des Datenintegritätsrisikos, wobei auf das Risikoprofil des Instituts abgestellt wird. Das Institut legt bspw. Rollen und Verantwortlichkeiten für die Verwaltung der Integrität der Daten (Dateneigentümer, Datenarchitekten) fest, dokumentiert die Datenarchitektur und Datenmodelle und führt Anwendungskontrollen durch. Schriftlich festgehalten sind zudem die Verfahren zur Datensicherung, die Anforderungen an die Verfügbarkeit (Verfahren zur Wiederherstellbarkeit), die Lesbarkeit (auch von Datensicherungen) und Aktualität der Daten sowie die für die Datenverarbeitung notwendigen IKT-Systeme. Auch in Hinblick auf ein funktionierendes Business Continuity Management (BCM) werden regelmäßige und anlassbezogene Tests durchgeführt, die die Verfahren für

[17] Grundsätzlich geht der Leitfaden davon aus, dass der IKT-Betrieb im eigenen Institut vor Ort angesiedelt ist. Im Falle von Auslagerungen bzw. Teilauslagerungen des IKT-Betriebs stellen die Institute sicher, dass die Vorgaben des § 25 BWG und dessen Anlage eingehalten werden.

eine erfolgreiche Datenwiederherstellung in angemessener Zeit prüfen und deren Funktionalität bestätigen.

10. IKT-AUSLAGERUNGEN

Mit 03.01.2018 ist § 25 BWG in Kraft getreten, wodurch eine nationale Rechtsgrundlage für Auslagerungen von Kreditinstituten und betrieblichen Vorsorgekassen eingeführt wurde. § 25 BWG enthält keine Definition des Begriffs „Auslagerung“, weshalb die in den CEBS GL on Outsourcing verwendete Definition heranzuziehen ist. Demzufolge gilt als „Auslagerung“ (Outsourcing) eine Vereinbarung jeglicher Form, die zwischen einem beaufsichtigten Institut und einem Dritten (Dienstleister) getroffen wird, bei dem es sich um ein beaufsichtigtes oder nichtbeaufsichtigtes Institut handeln kann, auf Grund derer der Dritte direkt oder durch weiteres Auslagern einen Prozess, eine Dienstleistung oder eine Tätigkeit erbringt, die ansonsten vom beaufsichtigten Institut selbst erbracht werden würde. Nicht unter den Begriff der Auslagerung fällt der Kauf von standardisierten Softwareprodukten inklusive Wartungsverträgen (sofern es sich nicht um eine Cloud-Lösung handelt).

Die Bestimmungen des § 25 BWG inkl. Anlage sind anzuwenden, wenn insbesondere aufgrund der durchgeführten Risikoanalyse das Auslagerungsvorhaben eine wesentliche bankbetriebliche Aufgabe im Sinne des § 25 Abs. 2 BWG umfasst. Institute legen zum Zweck dieser Wesentlichkeitsprüfung in ihrer Auslagerungs-Policy (oder als Teil der IKT-Strategie) konkret auf das jeweilige Geschäftsmodell bezogene Kriterien fest, anhand derer entschieden wird, ob eine wesentliche IKT-Auslagerung vorliegt. Im Falle einer wesentlichen IKT-Auslagerung ist das Auslagerungsvorhaben gem. § 25 Abs. 5 BWG der FMA anzuzeigen.[18] Erfasst sind einerseits neue Auslagerungsvorhaben, aber auch die Änderungen bestehender, vor dem 03.01.2018 abgeschlossener Auslagerungsvereinbarungen. Institute bringen diese Anzeige entsprechend der Art, dem Umfang und der Komplexität der geplanten Auslagerung frühzeitig vor dem geplanten Vertragsabschluss ein, um der FMA eine angemessene Einschätzung zu ermöglichen.[19]

[18] Zu diesem Zweck wurde auf der FMA Incoming Plattform [https://webhost.fma.gv.at/incomingplattform/ip.htm] im Menü „Bankwesengesetz“ ein neues Untermenü angelegt. In diesem Untermenü findet sich ein Anzeigeformular, das den Unternehmen zum Download bereitgestellt wird und in dem sämtliche aus Sicht der FMA für die Beurteilung eines Auslagerungsvorhabens relevanten Punkte abgefragt werden, sodass keine weiteren Begleitdokumente hochzuladen sind.

[19] Dadurch wird sichergestellt, dass der Aufsicht eine angemessene Zeit zur Überprüfung der Einhaltung der Auslagerungsbestimmungen zukommt und die Rückmeldung der FMA an das Institut vor Vertragsabschluss erfolgen kann. Sofern Sie die Auslagerungsvereinbarung schon vor dieser Rückmeldung rechtsverbindlich abschließen, ist nicht auszuschließen, dass diese erforderlichenfalls abzuändern oder aufzulösen ist, wenn den rechtlichen Anforderungen nicht entsprochen wird. Die Verantwortlichkeit für die Einhaltung der anzuwendenden Rechtsvorschriften verbleibt in jedem Fall beim auslagernden Institut.

Unbeschadet des § 25 BWG inkl. Anlage werden bei Auslagerungen die allgemeinen Regelungen des § 39 BWG berücksichtigt. Daraus wird bspw. abgeleitet, dass Institute sämtliche Auslagerungsvereinbarungen (sowohl wesentliche als auch nicht-wesentliche) schriftlich ausgestalten, um jederzeit eine Prüfung durch die internen Kontrollfunktionen, den Bankprüfer, die FMA oder die OeNB zu ermöglichen.

Darüber hinaus halten Institute insbesondere die Vorschriften gem. §§ 38[20], 39 Abs. 2a und 60 Abs. 3 BWG, § 11 KI-RMV sowie die in den CEBS Guidelines on Outsourcing (2006)[21] und die betreffend Auslagerungen in den EBA Leitlinien on Internal Governance[22] enthaltenen Bestimmungen ein.

Vorbehaltlich einer Compliance-Erklärung der FMA haben Institute hinsichtlich Auslagerungen an Cloud-Anbieter künftig die EBA recommendations on outsourcing to cloud service providers[23] zu beachten, welche ab dem 01.07.2018 gelten und auf den CEBS Guidelines on Outsourcing (2006) aufbauen. Die maßgeblichen Inhalte der EBA recommendations on outsourcing to cloud service providers sind die Wesentlichkeitsbewertung, die Pflicht zur angemessenen Unterrichtung der Aufsichtsbehörden (Bestimmungen zur Risikoanalyse und dem Informationsverzeichnis), die Regelung der Zugangs- und Prüfungsrechte, die Verpflichtungen hinsichtlich der Sicherheit von Daten und Systemen (Vertraulichkeit, Kontinuität, Qualität und laufende Überwachung der Leistung), die Bewertungskriterien für den Ort der Daten und Datenverarbeitung, Regelungen in Bezug auf Kettenauslagerungen sowie die Sicherstellung von Notfallplänen und Ausstiegsstrategien.

[20] Betreffend das gem. § 38 BWG einzuhaltende Bankgeheimnis sei auch auf die mit 25. April 2018 in Kraft tretende EU-Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) sowie das österreichische Datenschutz-Anpassungsgesetz 2018 verwiesen. Die damit eingeführten, hohen Strafrahmen stellen ein erhöhtes operationelles Risiko dar.

[21] Hinweis: Im aktuellen Arbeitsprogramm der EBA ist für das Jahr 2018 die Überarbeitung der CEBS Guidelines on Outsourcing vorgesehen [https://www.eba.europa.eu/documents/10180/1981573/EBA+2018+Work+Programme.pdf/].

[22] Hinweis: Derzeit sind die EBA GL 44 on internal governance [https://www.eba.europa.eu/documents/10180/103861/EBA_2012_00210000_DE_COR.pdf] in Kraft, es liegt jedoch bereits die finale Überarbeitung durch EBA vor (EBA/GL/2017/11) [https://www.eba.europa.eu/documents/10180/2164689/Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29_DE.pdf/], die vorbehaltlich der Compliance-Erklärung der FMA ab dem 30.06.2018 anzuwenden sind.

[23][https://www.eba.europa.eu/documents/10180/2170125/Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29_DE.pdf/]

11. VERFÜGBARKEIT UND KONTINUITÄT, NOTFALLMANAGEMENT

Unter Verfügbarkeits- und Kontinuitätsrisiko ist das Risiko aus Beeinträchtigungen der Leistung und Verfügbarkeit von IKT-Systemen zu verstehen. Insbesondere manifestiert sich das Risiko aus der mangelnden Fähigkeit der zeitkritischen Wiederherstellung von Leistungen, die aufgrund von Hardware- oder Softwareversagen geschädigt wurden, sowie durch allgemeine Schwächen im Management von IKT-Systemen. Institute legen für IKT-Systeme die „Recovery Time Objectives“ (RTO, d.h. die maximale Zeitspanne, innerhalb derer ein System oder ein Prozess nach einem Ereignis wiederhergestellt werden muss) und der „Recovery Point Objective“ (RPO, d.h. die maximale Zeitspanne, innerhalb derer Daten im Falle eines Ereignisses verloren gehen können) fest.

Ein Rahmenwerk zur Identifikation, Messung und Begrenzung des Verfügbarkeits- und Kontinuitätsrisikos ist daher implementiert. Dabei werden kritische Geschäftsprozesse, deren Abhängigkeiten und die dazu benötigten IKT-Ressourcen identifiziert, analysiert und in die geschäftlichen Ausfallsicherheits- und Kontinuitätspläne eingebunden.

Ein adäquates Notfallmanagement umfasst Strategien, Pläne, Handlungen und physische Maßnahmen zur Notfallvorsorge, Notfallbewältigung und Notfallnachsorge, um kritische Prozesse und Ressourcen bei unvorhergesehenen Unterbrechungen präventiv zu schützen und rasch wiederherzustellen.

Die Hauptaufgaben des Notfallmanagements sind zum einen, die Stabilisierung der Geschäftsprozesse, um die Wahrscheinlichkeit eines Zwischenfalls zu minimieren und zum anderen, die bestmögliche Vorbereitung auf Zwischen- oder Notfälle sicherzustellen. Dabei gewährleisten Geschäftsprozessfortführungs- und Wiederanlaufpläne, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen und innerhalb eines angemessenen Zeitraums der Normalbetrieb wieder ermöglicht wird.

Das Notfallmanagement fußt auf der Analyse der Bedrohungsanfälligkeiten von Geschäftsprozessen und -ressourcen und umfasst die präventive Notfallvorsorge und die Notfallbewältigung.

Die Festlegung von präventiven Maßnahmen, Sicherungs- und Wiederherstellungsverfahren, Störfallmanagement- und Eskalationsprozessen, Kapazitätsplanungslösungen in Richtlinien, Standards und operativen Kontrollen dienen der Schaffung eines adäquaten Rahmenwerks. Dabei ist zu beachten, dass die Verantwortung hinsichtlich ausgelagerter Aktivitäten im Institut verbleibt, sodass es in dessen Verantwortung liegt, dass ein Dienstleister über die entsprechenden Maßnahmen, Verfahren und Prozesse verfügt. Die festgelegten Maßnahmen sind dazu geeignet, das Ausmaß von Schäden zu reduzieren.

Die Kontinuität und Ausfallsicherheit der Notfallvorsorge ist ausreichend robust ausgestaltet und wird durch Notfallübungen regelmäßig überprüft, um eine rechtzeitige Wiederherstellung nach Betriebsstörungen zu gewährleisten. Die Notfallübungen müssen entsprechend geplant und dokumentiert werden.

Zur Erleichterung der Umsetzung des Notfallmanagements ist ein Koordinierungsgremium eingerichtet, dem Personen aus verschiedenen Organisationseinheiten angehören. Notfallpläne werden im Institut kommuniziert und entsprechende Schulungen durchgeführt. Beschrieben werden dabei Informationen zur direkten Notfallbewältigung, Kontaktinformationen und Handlungsanweisungen, welche im Notfall durchzuführen sind.

Im Fall einer Auslagerung verbleibt die Verantwortung für angemessene Notfallpläne in Bezug auf die ausgelagerten Tätigkeiten beim auslagernden Institut. Gleiches gilt für die Auslagerung von operativen Funktionen und Tätigkeiten. Dabei kommt der Dienstleister den festgelegten Notfallplananforderungen des Instituts nach. Notfallkonzepte sind aufeinander abgestimmt.