FMA

LEITFADEN

IT-Sicherheit in Kreditinstituten

ENTWURF

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 IT-Systeme von Unternehmen haben deutlich gemacht, wie verwundbar IT-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 Informationstechnologie (IT) resultieren, bewusst und sieht sich aufgrund der gestiegenen Risikolage einer intensivierten IT-Aufsicht verpflichtet. Aus diesem Grund wird den Instituten seitens der FMA ein Überblick über Ausgestaltung, Anforderungen und Vorkehrungen betreffend die IT-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 zur Orientierung herangezogen werden.

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 IT-Sicherheit, aufgrund der angebotenen Dienstleistungen, angemessen sind.

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 IT-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 IT-Sicherheit dargestellt:

- **Informationstechnologie bzw. Informationstechnik (IT)**
  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. Darunter wird auch Informations- und Kommunikationstechnologie verstanden.

- **IT-Risiko**
  ist das Geschäftsrisiko im Zusammenhang mit der Nutzung, dem Eigentum, dem Betrieb, der Beteiligung, der Einflussnahme und der Einführung von Informationstechnologie im Institut. Darunter kann das Risiko aus IT-Dienstleistungen, IT-Verfügbarkeit und -Kontinuität, IT-Sicherheit, IT-Änderungen, IT-Datenintegrität und IT-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 IT-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 (SREP) (EBA/GL/2017/05)[1], dem Basel Committee on Banking Supervision's standard number 239[2] und den CEBS Guidelines on Outsourcing[3].

[1] https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf
[2] https://www.bis.org/publ/bcbs239.pdf
[3] https://www.eba.europa.eu/documents/10180/104404/GL02OutsourcingGuidelines.pdf.pdf

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

- **ITIL**[4]
  Die IT Infrastructure Library (ITIL) ist ein etablierter Qualitätsstandard, indem sich vordefinierte Prozesse, Funktionen und Rollen für IT-Infrastrukturen von Unternehmen finden (Sammlung von Best Practices für Service Management).

- **BSI-Grundschutz**[5]
  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 IT-Umgebungen dienen.

- **CoBIT**[6]
  Das Rahmenwerk Control Objectives for Information and related Technology (CobiT) ermöglicht die Steuerung und Kontrolle des IT-Betriebs durch das Management. CobiT entstand aus einer Sammlung von mehreren IT-Standards, Rahmenwerken, Richtlinien und Best Practices

- **ISO 27001**[7]
  Die ISO 27001 wurde erarbeitet für die Einrichtung, Implementierung, Wartung und laufende Verbesserung eines Informationssicherheitsmanagementsystems.

- **Österreichisches Informationssicherheitshandbuch**[8]
  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.etc.at/itil/
[5] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
[6] http://www.isaca.org/cobit/pages/default.aspx
[7] https://www.iso.org/standard/54534.html
[8] https://www.sicherheitshandbuch.gv.at/

2. IT-STRATEGIE

Geschäftsleiter von Instituten erstellen eine mit der Geschäftsstrategie übereinstimmenden IT-Strategie, welche im Einklang mit Art, Umfang und Komplexität der IT-Tätigkeiten steht.

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

Die IT-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 IT-Strategie wird ein unternehmens- und gruppenweites Bewusstsein für Informationssicherheit geschaffen und deren Berücksichtigung in den jeweiligen Fachbereichen verankert. Dies erfolgt bspw. durch: Kommunikation auf Gruppenebene, entsprechende Trainings, Maßnahmen zur Bewusstseinsbildung der Mitarbeiter.

Zu beachten ist dabei, dass die IT-Strategie eine wichtige Informationsquelle für die IT-Revision und für die Einbindung der IT in die Ertrags- und Risikosteuerung ist. Daher enthält die IT-Strategie auch Aussagen zur geplanten Ausgestaltung der IT, wodurch Planungssicherheit für die IT-Organisation, taktische IT-Planung und Ressourcenplanung ermöglicht wird.

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

In der IT-Strategie werden die strategische Entwicklung, der IT-Aufbau- und Ablauforganisation inklusive der dazugehörigen Prozesse, festgelegt. Hierbei orientieren sich die Institute an bestehenden Standards (z.B. ISO 27001, BSI-Grundschutz). Des Weiteren werden bspw. folgende Punkte in die IT-Strategie aufgenommen:

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

- Festlegung der Grundsätze eines Lebenszyklus-Managements von Hard- 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. IT-GOVERNANCE

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

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

Die Geschäftsleitung stattet das IT-Risikomanagement (insb. Informationsrisikomanagement, Informationssicherheitsmanagement, IT-Betrieb und Anwendungsentwicklung) entsprechend der Art, dem Umfang, der Komplexität der betriebenen Bankgeschäfte und unter Berücksichtigung der aktuellen und zukünftigen Risikosituation quantitativ und qualitativ angemessen mit Personal aus.

Institute verfügen über Prozesse zur Identifikation, Bewertung, Steuerung und Überwachung der wesentlichen IT-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 IT-Risiken.

Abschließend ist festzuhalten, dass die Unternehmensführung ausreichende Ressourcen für die Behandlung von IT-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, IT-Risiken und deren Behandlung in adäquater Weise.

4. INFORMATIONSRISIKOMANAGEMENT

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

Das Informationsrisikomanagement gewährleistet daher, dass die Informationsverarbeitung und -weitergabe im Institut durch adäquate IT-Systeme (Hardware- 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 Risikobewertung durchgeführt, sodass alle relevanten Informationen des Unternehmens entsprechend berücksichtigt werden.

Im Zuge der Etablierung eines Informationsrisikomanagementsystems im Institut werden Interessenskonflikte vermieden. Zudem wird die Berücksichtigung von Schnittstellen und Abhängigkeiten von geschäftsrelevanten Informationen, Geschäftsprozessen, IT-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. Des Weiteren ist ein präventiver Maßnahmenkatalog zur Reduzierung der Informationsrisiken 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.

5. SCHUTZMAßNAHMEN/SICHERHEITSMANAGEMENT

Das Institut verfügt über Prozesse zum IT-Risikomanagement und etabliert adäquate Schutzmaßnahmen zur IT-Risikobegrenzung. Zentraler Bedeutung kommt dabei dem Schutz von Informationen (Informationssicherheitsmanagement), der Vergabe von Berechtigungen (Benutzerberechtigungsmanagement), aber auch dem Schutz von Daten zu (Datensicherung, etc.).

5.1. INFORMATIONSSICHERHEITSMANAGEMENT

Das Institut etabliert Prozesse, welche den Schutz von Informationen gewährleisten (z.B. Informationssicherheitsrichtlinie). Diese werden von der Geschäftsleitung beschlossen und angemessen im Institut 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).

Die Informationssicherheitsrichtlinie ist Ausgangspunkt für konkretisierende Richtlinien und Prozesse für Teilbereiche, wie bspw. Netzwerksicherheit, Kryptografie, Authentisierung, Protokollierung, etc. Dabei werden Schutzmaßnahmen, Methoden zur Identifikation, Reaktionen und Wiederherstellungsabläufe bei Sicherheitsvorfällen definiert.

Das Institut richtet aufgrund der Art, dem Umfang, 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 gegenüber Dritten und die Überprüfung und Überwachung der Einhaltung der Informationssicherheitsprozesse und -richtlinien ist. 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 IT-Relevanz sowie die Untersuchung von Sicherheitsvorfällen. Zudem steht der Informationssicherheitsbeauftragte mit seiner Expertise betroffenen Abteilungen zur Verfügung.

Die Funktion des Informationssicherheitsbeauftragten ist organisatorisch und prozessual unabhängig ausgestaltet und im eigenen Institut vor Ort etabliert. Institute können im Rahmen eines Sektorverbundes ohne wesentliche eigenbetriebene IT auch einen gemeinsamen Informationssicherheitsbeauftragten bestellen, wobei dem Informationssicherheitsbeauftragten 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.

5.2. BENUTZERBERECHTIGUNGSMANAGEMENT

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

Ziel des Benutzerberechtigungsmanagements ist es, dass nur autorisierte Benutzer im Institut auf IT-Services und -Anwendungen zugreifen können. Damit dient es insbesondere der Hintanhaltung missbräuchlicher Verwendung und unautorisierter Manipulation von Daten und IT-Systemen.

Das Institut verfügt über ein dokumentiertes Berechtigungskonzept bzw. Benutzerberechtigungsprozesse. Die Vergabekriterien von Berechtigungen berücksichtigen dabei den Grundsatz der minimalen Rechtevergabe bzw. das Need-to-know-Prinzip und sind nachvollziehbar sowie konsistent. Zudem werden Funktionstrennungen gewahrt und Interessenskonflikte vermieden.

Das gemeinsame Verwenden von Zugangsdaten (z.B. bei Webapplikationen) 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. Eingeräumte Berechtigungen werden regelmäßig überprüft, ob sie dem Berechtigungskonzept bzw. den -prozessen entsprechen, nur wie vorgesehen eingesetzt werden und 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.

5.3. SCHWACHSTELLENMANAGEMENT

Schwachstellenmanagement als integraler Bestandteil der Computer- und Netzsicherheit 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 Schadenssoftware ist heutzutage nicht mehr ausreichend, weshalb zusätzliche Schutzmaßnahmen getroffen werden. Dazu gehören bspw.:

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

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

6. IT-PROJEKTE UND ANWENDUNGSENTWICKLUNG

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

Um mögliche Beeinträchtigungen des Risikoprofils des Instituts identifizieren zu können, werden IT-Projekte angemessen gesteuert, deren Risiken laufend berücksichtigt und dies vollständig dokumentiert. Institute überwachen und steuern die festgelegten Vorgehensmodelle bei IT-Projekten und deren Portfolio angemessen. Grundvoraussetzung dafür ist die Führung einer Inventarliste über die IT-Ressourcen. Der Geschäftsleitung werden wesentliche IT-Projekte und deren Risiken in regelmäßigen Intervallen und anlassbezogen berichtet. Im Rahmen

ihrer Aufgaben erfolgt die Einbeziehung von einzelnen Organisationseinheiten des Instituts an den IT-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 nachvollziehbar und vollständig dokumentiert, um etwaigen Manipulationen vorzubeugen (Software-Quellcode-Kontrollsystem). In diesem Zusammenhang wird auf die jederzeitige Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten – bereits vor der Produktion bis hin zum Austausch, Archivieren, Entsorgen oder Vernichten von Anwendungen – geachtet (Sicherheitslücken-Screening).

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. Diese geben die Produktionsumgebung effizient wieder. Die Produktivsetzung von System- bzw. Anwendungsänderungen erfolgen erst nach ausführlichen Tests, um etwaige Störungen des Geschäftsbetriebs zu verhindern. 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 IT-Systeme, 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 erstellt.

In Bezug auf menschliches Fehlverhalten verfügt das Institut über einen unabhängigen Überprüfungs- und Validierungsprozess, um eine maximal mögliche Reduktion der Risiken bei der Durchführung von Änderungen an IT-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.

7. IT-BETRIEB UND DATENINTEGRITÄT

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

Institute verwalten die IT-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. Zudem bestehen Prozesse zur Neu- bzw. Ersatzbeschaffung sowie Nachbesserung unter Berücksichtigung möglicher Umsetzungsrisiken.

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 Datenintegritätrisikos, wobei auf das Risikoprofil des Instituts abzustellen ist. Schriftlich festzuhalten ist demnach 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 IT-Systeme. Auch in Hinblick auf ein funktionierendes Business Continuity Management (BCM) werden regelmäßige und anlassbezogene Tests durchgeführt, die die Verfahren für eine erfolgreiche Datenwiederherstellung in angemessener Zeit prüfen und deren Funktionalität bestätigen.

8. IT-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. Erfasst sind einerseits neue Auslagerungsvorhaben, aber auch die Änderungen bestehender, vor dem 03.01.2018 abgeschlossenen Auslagerungsvereinbarungen. Institute legen zum Zweck dieser Wesentlichkeitsprüfung in ihrer Auslagerungs-Policy (oder als Teil der IT-Strategie) konkret auf das jeweilige Geschäftsmodell bezogene Kriterien fest, anhand derer entschieden wird, ob eine wesentliche IT-Auslagerung vorliegt. Im Falle einer wesentlichen IT-Auslagerung ist das Auslagerungsvorhaben gem. § 25 Abs. 5 BWG der FMA anzuzeigen[9]. Institute bringen diese Anzeige entsprechend der Art, Umfang und Komplexität der geplanten Auslagerung rechtzeitig vor dem geplanten Vertragsabschluss ein. 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.[10]

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 die Vorschriften gem. §§ 38[11], 39 Abs. 2a und 60 Abs. 3 BWG, § 11 KI-RMV sowie die in den CEBS Guidelines on Outsourcing (2006) und die betreffend Auslagerungen in den EBA Leitlinien on Internal Governance[12] enthaltenen Bestimmungen ein.

---

[9] 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.

[10] 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.

[11] 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.

[12] 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 in der englischen Fassung vor (EBA/GL/2017/11) [https://www.eba.europa.eu/documents/10180/1972987/Final+Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29.pdf], die vorbehaltlich der Compliance-Erklärung der FMA ab dem

Vorbehaltlich einer Compliance-Erklärung der FMA haben Institute hinsichtlich Auslagerungen an Cloud-Anbieter künftig die EBA recommendations on outsourcing to cloud service providers 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.

9. VERFÜGBARKEIT UND KONTINUITÄT, NOTFALLMANAGEMENT

Unter Verfügbarkeits- und Kontinuitätsrisiko ist das Risiko aus Beeinträchtigungen der Leistung und Verfügbarkeit von IT-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 IT-Systemen.

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

Ein adäquates Notfallmanagement umfasst Strategien, Pläne und Handlungen 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 Schadenszwischenfalls zu minimieren und zum anderen, die bestmögliche Vorbereitung auf Zwischen- oder Notfälle sicherzustellen. Dabei gewährleisten Geschäftsfortführungs- und Wiederanlaufpläne, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen und innerhalb eines angemessenen Zeitraums der Normalbetrieb wieder ermöglicht wird.

30.06.2018 anzuwenden sind. Ebenfalls sind auch die EBA Recommendations on outsourcing to cloud service providers (EBA/Rec/2017/03) [https://www.eba.europa.eu/documents/10180/1712868/Final+draft+Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29.pdf]vorbehaltlich einer Compliance-Erklärung durch die FMA ab dem 01.07.2018 zu berücksichtigen.

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 dient der Schaffung eines adäquaten Rahmenwerks. Die festgelegten Maßnahmen sind dazu geeignet, das Ausmaß von Schäden zu reduzieren.

Die Kontinuität und Ausfallsicherheit der IT ist ausreichend robust ausgestaltet und wird durch Testläufe überprüft, um eine rechtzeitige Wiederherstellung nach Betriebsstörungen zu gewährleisten.

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.

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