FMA

Dokumentennummer: 05 / 2018
Veröffentlichungsdatum: 19.12.2018

FMA-LEITFADEN IT-SICHERHEIT

FÜR PENSIONSKASSEN

INHALTSVERZEICHNIS

ZIELSETZUNG UND HINWEISE

Die zunehmende Digitalisierung birgt – neben vielen Vorteilen im Wirtschaftsleben – neue Gefahren und Risiken, denen Unternehmen, einschließlich Pensionskassen (PK), ausgesetzt sind. Auch für PK, 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 PK seitens der FMA ein Überblick über Ausgestaltung, Anforderungen und Vorkehrungen betreffend die IT-Sicherheit von PK als Orientierungshilfe zur Verfügung gestellt.

Dieser Leitfaden richtet sich an alle von der FMA beaufsichtigten PK.

Dieser Leitfaden stellt keine Verordnung dar. Er soll für die beaufsichtigten PK 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.

Die Ausführungen in diesem Leitfaden sind unter dem Grundsatz der Proportionalität zu sehen. Nach diesem Grundsatz entsprechen Anwendungen der Wesensart, dem Umfang und der Komplexität der mit der Tätigkeit der PK einhergehenden Risiken. Dabei bestimmt die jeweilige PK selbst, welche Methoden, Systeme und Prozesse in Bezug auf die IT-Sicherheit angemessen sind. Die rechtlichen Grundlagen bleiben durch diesen Leitfaden unberührt

I. RECHTSGRUNDLAGEN

Dieser Leitfaden basiert insbesondere auf § 21a PKG[1] (Risikomanagement und Risikomanagementfunktion) und § 22a PKG (Eigene Risikobeurteilung). Bei der Behandlung von IT-Risiken können die Pensionskassen auf etwaige etablierte Standards zurückzugreifen. Dazu gehören etwa:

- *ISO 27001:*[2]
  Die ISO 2700X-Reihe ist eine Reihe von Standards der IT-Sicherheit. Beispielsweise wurde die ISO 27001 für die Einrichtung, Implementierung, Wartung und laufende Verbesserung eines Informationssicherheitsmanagementsystems erarbeitet.
- *Österreichisches Informationssicherheitshandbuch:*[3]
  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 ISO 27001-Umsetzung.
- *ITIL:*[4]
  Die IT Infrastructure Library (ITIL) ist ein etablierter Qualitätsstandard, der vordefinierte Prozesse, Funktionen und Rollen für IT-Infrastrukturen von Unternehmen umfasst (Sammlung von Best Practices für Service Management).
- *COBIT:*[5]
  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.
- *BSI-Grundschutz:*[6]
  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.

[1] Die Rechtsgrundlage basiert auf der PKG-Novelle vom 30.11.2018 (BGBl I Nr. 81/2018)
[2] https://www.iso.org/standard/54534.html.
[3] https://www.sicherheitshandbuch.gv.at.
[4] Siehe z.B. https://www.etc.at/itil/ oder https://www.axelos.com/best-practice-solutions/itil.
[5] https://www.isaca.org/cobit/pages/default.aspx.
[6] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html.

II. DEFINITIONEN

Für Zwecke dieses Leitfadens werden nachstehend die maßgeblichen Definitionen in Bezug auf die IT-Sicherheit dargestellt. Im Übrigen werden grundsätzlich die Definitionen der ISO-Standards verwendet.

- *IT:*
  Sie umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören insbesondere die Erhebung, die Erfassung, die Nutzung, die Speicherung, die Übermittlung, die programmgesteuerte Verarbeitung, die interne Darstellung und die Ausgabe von Informationen.

- *IT-Risiko:*[7]
  Dieses 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 der IT-Verfügbarkeit und -Kontinuität, der IT-Sicherheit, der IT-Änderungen, der IT-Datenintegrität und der IT-Auslagerungen fallen.

III. GOVERNANCE

A. ROLLE DES VORSTANDS

Der Vorstand stellt bezüglich der IT-Sicherheit die Einhaltung der für den Betrieb des PK-Geschäfts geltenden Vorschriften sicher. Dies umfasst unter anderem

- die Festlegung, Überprüfung und gegebenenfalls die Anpassung der IT-Strategie,
- die Festlegung, Umsetzung und die bei Bedarf erfolgende zeitnahe Anpassung der IT-Aufbau- und Ablauforganisation,
- die Festlegung von Kriterien zur Steuerung der IT (beispielsweise betreffend die Verfügbarkeit, die Anpassungsfähigkeit an neue Anforderungen, die generelle Qualität),
- Beschluss von schriftlichen IT-Risikomanagementleitlinien (als Teil der Risikomanagementleitlinien) und Vorgaben zur Informationssicherheit,
- Gewährleistung der Kohärenz der Strategien und Verfahren zum IT-Risiko mit den strategischen Unternehmenszielen.

[7] Bei den synonymen Begriffen „IT-Risiko“, „Informations- und Kommunikationstechnologie (IKT)-Risiko“ bzw. „Informationssystemrisiko“ wird das gleiche Risiko adressiert.

B. IT-STRATEGIE

Die IT-Strategie und die Geschäftsstrategie sind aufeinander abgestimmt. Die IT-Strategie umfasst insbesondere

- die strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation, insbesondere im Hinblick auf Personaleinsatz und Budget,
- einen Überblick über die geplante Anwendungslandschaft,
- die Festlegung von Standards, an denen sich die PK orientiert, unter Darlegung des aktuellen und des geplanten Umsetzungsgrades,
- die grundsätzliche Herangehensweise zur Berücksichtigung der Informationssicherheit in der Unternehmensorganisation,
- eine Grundsatzstrategie zum IT-Notfallmanagement,
- eine Positionierung zur Zulässigkeit und zu Voraussetzungen bezüglich dem lokalen Einsatz spezifischer IT-Systeme (Hard- und Software-Komponenten) in den einzelnen Organisationseinheiten,
- die Grundsätze eines Lebenszyklus-Managements von Hard- und Software.

Die IT-Strategie ist innerhalb eines angemessenen Zeitraums an Änderungen der strategischen Ziele, der Geschäftstätigkeit, des Geschäftsumfelds oder der Risikolage der PK anzupassen. Das Risikobewusstsein der Mitarbeiter für das IT-Risiko wird im gesamten Unternehmen geschult.

C. IT-GOVERNANCE

Die auf der IT-Strategie basierende IT-Governance gewährleistet einen ordnungsgemäßen Betrieb sowie bei Bedarf erfolgende Anpassungen der IT-Systeme und -Prozesse. Die **technisch-organisatorische Ausstattung** ist angemessen und entspricht den vom Vorstand vorgegebenen Kriterien, die auf der IT-Strategie basieren. Die PK stattet sich bezüglich der IT-spezifischen Anforderungen mit quantitativ und qualitativ angemessenen Personalressourcen aus.

Interessenkonflikte innerhalb der IT-Aufbau- und Ablauforganisation werden vermieden bzw. adäquat adressiert werden. Klar abgegrenzte Rollen und Verantwortlichkeiten für Identifikation, Beurteilung, Monitoring, Minimierung, Reporting und Beaufsichtigung der wesentlichen IT-Risiken werden definiert.

Die IT-Governance unterliegt einer regelmäßigen internen Überprüfung.

Im Fall von Auslagerungen der IT-Dienstleistungen sind die Vorgaben des § 11h PKG zu beachten.

IV. STEUERUNG

A. RISIKOMANAGEMENT VON IT-RISIKEN

IT-Risiken werden im Rahmen des Risikomanagements operationeller Risiken bzw. der eigenen Risikobeurteilung behandelt. Risiken zur Informationsverarbeitung, -weitergabe und -speicherung, welche durch adäquate IT-Systeme und -Prozesse unterstützt sind, werden abgedeckt. Ein Überblick über den Informationsverbund, der beispielsweise Informationen, IT-Systeme, Netz- und Gebäudeinfrastrukturen sowie Schnittstellen umfasst, erleichtert das Risikomanagement von IT-Risiken.

Die auf IT-Risiken bezogene Risikobeurteilung durchläuft die folgenden Prozessschritte:

- *Risikoidentifikation:*

Mögliche Ursachen für IT-Risiken sind:

- inadäquate Absicherung der Schnittstellen zum Internet,
- unzureichende Maßnahmen zur Förderung des Risikobewusstseins der Mitarbeiter,
- Auslagerungen,
- wesentliche Änderungen bzw. Umstellungen des IT-Systems, der IT-Prozesse oder von IT-Funktionen.

Im Rahmen der Risikokategorisierung werden auch die identifizierten IT-Risiken beschrieben und systematisiert dargestellt. Der notwendige Detaillierungsgrad hängt von den unternehmensspezifischen Gegebenheiten ab.

- Die durch die Eintrittswahrscheinlichkeit und das Schadensausmaß determinierte **Risikoanalyse** bildet die Basis für die **Risikobewertung**, welche etwa über eine Risikomatrix abgebildet wird. Insbesondere Cyberrisiken werden beispielsweise durch die Durchführung von Penetrationstests (Ausnutzen von Software-Schwachstellen und Sicherheitslücken in der IT-Infrastruktur, um unberechtigten Zugang zu dieser zu erhalten) adressiert.
- Zur angemessenen **Risikosteuerung** verfügt die PK über eine Methodik zur Ermittlung des Schutzbedarfs der Komponenten des Informationsverbunds. Insbesondere auf die Schutzziele Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität von Informationen wird dabei abgestellt. Auch Erkenntnisse aus dem Notfallmanagement werden dabei berücksichtigt. In Abhängigkeit von der Schutzbedarfskategorie werden Maßnahmenkataloge zur Risikomitigation festgelegt und umgesetzt.

  Mögliche Maßnahmen sind:
  - der grundsätzliche Ersatz manueller durch automatisierte Schnittstellen,
  - die Protokollierung von Benutzer- und Administratorentätigkeiten,
  - Passwortvorgaben z.B. zur Passwortlänge und -zusammensetzung, zur Sicherstellung eines notwendigen Sicherheitsniveaus für den Einsatz von Benutzername/Passwort-Verfahren,
  - Umschaltung auf einen Ersatzrechner bei Ausfall des Verwaltungsservers.

Das von der PK bewusst übernommene IT-Restrisiko ist transparent dargestellt.

- **Risikoberichte** enthalten auch Ausführungen zum Risikomanagement von IT-Risiken.

B. INFORMATIONSSICHERHEITSMANAGEMENT

Zum Schutz von Informationen sind Prozesse etabliert und deren Umsetzung gesteuert. Informationssicherheit bezieht sich insbesondere auf die Aspekte

- Integrität, d.h. Informationen können nur von den vorgesehenen Personen und Prozessen verändert werden,
- Vertraulichkeit, d.h. Informationen können nur für die vorgesehenen Personen und Prozesse offen gelegt werden,
- Verfügbarkeit, d.h. Informationen werden für die vorgesehenen Personen und Prozesse verlässlich bereitgestellt, wenn diese sie benötigen,
- Authentizität, d.h. Informationen sind stets verlässlich und überprüfbar.

Die konkreten Ziele und der Geltungsbereich des Informationssicherheitsmanagements werden festgelegt. Dabei wird der im Rahmen des Managements von IT-Risiken definierte Schutzbedarf konkretisiert.

Die zur Erfüllung der Informationssicherheitsziele ergriffenen **Sicherheitsmaßnahmen** umfassen insbesondere technische Sicherheitsmaßnahmen und organisatorische Abläufe und Prozesse. Mögliche Beispiele sind:

- Schulungen zur Informationssicherheit,
- Datensicherungen und regelmäßige Überprüfung der Funktionalität der Datensicherung (Backup und Restore),
- zentrale und dezentrale Anti-Virus Scans,
- Intrusion Detection/Prevention Systeme (z.B. Überprüfen der Logdaten auf Cyberattacken, laufende Überprüfung der Firewall-Konzepte unter Zuhilfenahme interner oder externer Prüfmethoden, wie z.B. Port-Scans),
- systematisiertes Patchmanagement,
- Evaluierung von Sicherheitsmaßnahmen insbesondere bezüglich neuer Technologien (z.B. hinsichtlich der Verwendung von Cloud-Services, aber auch im Hinblick auf neue Arten von Cyberattacken).

Nach Sicherheitsvorfällen werden die Auswirkungen auf die Informationssicherheit analysiert und angemessene Nachsorgemaßnahmen veranlasst. Aufgrund der laufend steigenden Bedeutung der IT und der zunehmenden Informationsvernetzungen kommt der Organisation des Informationssicherheitsmanagements als **kontinuierlichem Verbesserungsprozess** hohe Bedeutung zu.

Das Erfordernis der Ernennung eines Informationssicherheitsbeauftragten, der alle Belange der Informationssicherheit innerhalb der PK und gegenüber Dritten wahrnimmt, wird stets auf Basis der Evaluierungserkenntnisse geprüft. In diesem Fall sind Rollen und Verantwortlichkeiten klar zu verteilen und Interessenskonflikte zu adressierenund insbesondere die laufende Information und Beratung des Vorstands zu gewährleisten.

C. IT-NOTFALLMANAGEMENT

IT-Risiken sind mit dem Risiko der Betriebsunterbrechung eng verknüpft. Zweck des IT-Notfallmanagements (Business Continuity Management) ist das Treffen angemessener Vorkehrungen, um die Kontinuität und Ordnungsmäßigkeit der IT-unterstützten Tätigkeiten der PK zu gewährleisten. Generell stellt das Notfallmanagement sicher, dass bei einer unvorhergesehenen Störung von Systemen und Verfahren, wesentliche Daten und Funktionen erhalten bleiben und die PK-Tätigkeiten fortgeführt werden oder – sollte dies nicht möglich sein – die entsprechenden Daten und Funktionen zeitnah wiederhergestellt und der Betrieb der PK rasch wiederaufgenommen werden. Durch ein angemessenes Notfallmanagement werden die Widerstandsfähigkeit zeitkritischer Geschäftsprozesse des Unternehmens und die Kontinuität der PK erhöht und somit auch die Interessen der Anwartschafts- und Leistungsberechtigten an einer kontinuierlichen Leistungserbringung geschützt.

Zur organisatorischen Umsetzung des Notfallmanagements wird ein Koordinierungsgremium eingerichtet, dem Personen aus verschiedenen Organisationseinheiten angehören (**Notfallteam**).

Die **Phasen** des Notfallmanagements:

- **Entwicklung:**
  - Im Rahmen der **Business Impact Analyse** (BIA) werden zeitkritische Geschäftsprozesse, deren Abhängigkeiten und die dazu benötigten IT-Ressourcen identifiziert, um diese in Folge besonders absichern zu können. Dafür werden Auswirkungen von Ressourcen- (jedenfalls IT-Systeme, Daten, Personal und Vertragspartner) bzw. Geschäftsprozessausfällen eingeschätzt. Eine Einstufung als „kritisch“ wird im Hinblick auf die Erreichung der (primären) Unternehmensziele und die jeweilige Zeitsensitivität bezüglich der Priorität in der Wiederherstellung vorgenommen.
  - Die **Risikoanalyse**, welche auf etablierte Prozesse des Risikomanagements zurückgreift, dient der Bewertung von Gefährdungen, welche durch das Zusammenwirken von Bedrohungen zur Unterbrechung von Geschäftsprozessen und Schwachstellen entstehen. Die signifikantesten Risiken für die PK werden genau definiert und priorisiert. Bei der Durchführung der Risikoanalyse wird auf die – in der BIA ermittelten – zeitkritischen IT-Prozesse und -Ressourcen abgestellt. Ein breites Spektrum von IT-Notfällen ist berücksichtigt. Diesbezügliche Beispiele sind Cyberattacken, Schadprogramme, Datendiebstähle, Risiken im Zusammenhang mit der Nutzung von Cloud-Leistungen oder die Nutzung von Sicherheitslücken zum unberechtigten Zugang der IT-Infrastruktur.

  - Auf Basis der BIA und der Risikoanalyse werden anschließend IT-spezifische **Notfallplanstrategien** festgelegt. Strategien, die von der vollständigen Aufrechterhaltung der IT-Prozesse und -Ressourcen bis hin zu einem Absehen von Maßnahmensetzungen reichen, hängen auch von Kosten-/Nutzenüberlegungen ab. IT-Notfallplanstrategien sind in **IT-Notfallplänen**, welche die Vorgehensweisen, Ersatzlösungen und die dafür benötigten Ersatzressourcen für die Wiederherstellung bzw. die Fortsetzung der kritischen Prozesse beschreiben, festgelegt.

- **Implementierung:**
  - Bewusstseinsbildungen und **Schulungen** zum IT-Notfallmanagement werden durchgeführt.
  - Regelmäßige – zumindest jährliche – **Tests** von IT-Notfallplänen werden durchgeführt. Bei Prozessänderungen oder bei neuen wesentlichen Bedrohungen werden zudem Tests ad-hoc durchlaufen.
- **Wartung und Aktualisierung:**
  - Anpassungen von Notfallplänen werden auf Basis der Erkenntnisse der IT-Notfallplantests vorgenommen.

V. OPERATIVE UMSETZUNG

A. IT-BETRIEB

Der IT-Betrieb hat die Aufgabe, 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 einer PK ergeben sich aus der Geschäftsstrategie und lassen sich aus den IT-unterstützten Geschäftsprozessen ableiten.

Zur adäquaten Berücksichtigung der Risiken alternder IT-Systeme werden deren Lebenszyklen überwacht und gemanagt. Zu diesem Zweck ist ein **Inventar bezüglich aller IT-Systeme**, sowie deren Beziehungen, Abhängigkeiten und Schnittstellen vorhanden. Prozesse zur Neu- bzw. Ersatzbeschaffung sowie zu Nachbesserungen bestehen, wobei mögliche Umsetzungsrisiken berücksichtigt werden. Zudem stellen PK die laufende Wartung ihrer IT-Systeme sicher – entsprechende Wartungsverträge sind vorhanden.

Ein **Prozess zum Umgang mit Störungen** sowie zu deren Ursachenerfassungen ist festgelegt. Beispielsweise sind mögliche Korrelationen von Störungen und deren Ursachen, die Vorgehensweise der Bearbeitung, Ursachenanalyse, Lösungsfindung und Nachverfolgung erfasst.

Ein im Einklang mit dem Notfallmanagement und den Geschäftsprozessen stehendes **Datensicherungskonzept** wird vorgegeben. Test zur Wiederherstellbarkeit und Lesbarkeit von Datensicherungen werden regelmäßig und anlassbezogen durchgeführt.

B. BENUTZERBERECHTIGUNGEN

Die Vergabe von Benutzerberechtigungen entspricht dem **Need-to-know-Prinzip,** dem im Falle von Auslagerungen eine besondere Bedeutung zukommt. Dabei ist für die PK selbst und die FMA ein jederzeitiger Zugang zu den Informationen über die ausgelagerten Tätigkeiten sichergestellt (§ 11h PKG).

Zur Verhinderung von Berechtigungsumgehungen werden **präventive Maßnahmen** getroffen. Die Protokollierung von Benutzer- und Administratorentätigkeiten beugt etwa allfälligen Datenmanipulationen vor. Erteilte Berechtigungen werden hinsichtlich der vorgesehenen Verwendung regelmäßig überprüft und gegebenenfalls angepasst.

Das Benutzerberechtigungskonzept und die technischen Benutzerberechtigungssysteme stehen mit dem unternehmensspezifischen Risikoprofil im Einklang.

C. IT-PROJEKTE, ANWENDUNGSENTWICKLUNGEN UND ZUGEKAUFTE SOFTWARE[8]

Die PK verfügt über eine Gesamtübersicht über alle wesentlichen IT-Projekte und Anwendungsentwicklungen. Bei der Umsetzung wird auf Folgendes geachtet:

- Wesentliche **IT-Projekte** werden vorab – insbesondere unter Einbezug der Risikomanagement-Funktion – auf deren Auswirkungen auf die IT-Aufbau- und IT-Ablauforganisation sowie die dazugehörigen IT-Prozesse untersucht. Ein adäquates Risikocontrolling wird eingerichtet. Besonders bei Einsatz vergleichsweise alter IT-Infrastruktur nimmt die Steuerung von IT-Projekten einen hohen Stellenwert ein. Deshalb werden wesentliche IT-Projekte und deren Risiken dem Vorstand regelmäßig und auch anlassbezogen berichtet.
- **Anwendungen** und **Anwendungsentwicklungen** werden nachvollziehbar dokumentiert. Für Anwendungsentwicklungen – beispielsweise für die Entwicklung individueller Softwarekomponenten – werden angemessene Prozesse festgelegt. Diese umfassen ein System zur Anforderungsgenerierung in den Organisationseinheiten, die technische Umsetzung sowie einen geregelten Test- und Abnahmeprozess. Vor dem erstmaligen Einsatz im Echtbetrieb bzw. nach wesentlichen Änderungen werden Anwendungen auf deren Funktionalität, auf Sicherheitskontrollen sowie auf Systemleistungen in unterstellten Stresssituationen getestet.

  Auf die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten wird bereits im Stadium der Anwendungsentwicklung geachtet.

  Anwendungen werden im laufenden Betrieb auf mögliche Mängel überwacht, auf deren Ursachen untersucht und bei Bedarf nachgebessert.

[8] Die nachstehenden Ausführungen betreffen sinngemäß auch zugekaufte Software.