FMA

Finanzmarktaufsicht
Liechtenstein

FMA-Richtlinie 2021/3 – Richtlinie IKT-Sicherheit

Richtlinie betreffend die Überwachung von Informations- und Kommunikationstechnologie (IKT) -Risiken

Referenz:	FMA-RL 2021/3
Adressaten:	- Banken nach BankG - Wertpapierfirmen nach BankG - E-Geld-Institute nach EGG - Zahlungsinstitute nach ZDG - Versicherungsunternehmen nach VersAG - Versicherungsvermittler nach VersVertG - Vorsorgeeinrichtungen nach BPVG - Pensionsfonds nach PFG - Verwaltungsgesellschaften und OGAW nach UCITSG - Verwaltungsgesellschaften und Investmentunternehmen nach IUG 2015 - Verwalter alternativer Investmentfonds nach AIFMG - Vermögensverwalter nach VVG
Publikation:	Website
Erlass:	19. Mai 2021
Inkraftsetzung:	1. Januar 2022
Letzte Änderung:	-
Rechtliche Grundlagen:	Art. 4 FMAG, Art. 25 Abs. 1 FMAG

Landstrasse 109 • Postfach 279 • 9490 Vaduz • Liechtenstein
Telefon +423 236 73 73 • Telefax +423 236 73 74 • www.fma-li.li • info@fma-li.li

FMA

Inhaltsverzeichnis

1. Grundsätze und Rechtsgrundlagen

1. Diese Richtlinie stützt sich auf die Art. 4 und 25 des Finanzmarktaufsichtsgesetzes (FMAG). Diese Rechtsgrundlagen werden durch spezialgesetzliche Regelungen ergänzt.[1]
2. Die Richtlinie IKT-Sicherheit ist vor dem Hintergrund des Prinzips der Proportionalität zu sehen. Die Umsetzung der Richtlinie richtet sich nach der jeweiligen Risikostruktur, der Komplexität, der Grösse, dem Umfang sowie der Art des Geschäfts eines Finanzintermediärs. Die angemessene Umsetzung ist durch den Finanzintermediär sicherzustellen.
3. Finanzintermediäre müssen nebst den Anforderungen dieser Richtlinie auch die für sie jeweils geltenden aufsichtsrechtlichen Anforderungen beachten. Deren konkrete Anwendbarkeit bestimmt sich nach den auf der FMA-Webseite publizierten FMA-Mitteilungen bzgl. Anwendung der von den Europäischen Aufsichtsbehörden herausgegebenen Leitlinien und Empfehlungen.[2]
4. Anforderungen an Funktionen, für welche keine gesetzliche Grundlage besteht, müssen nicht umgesetzt werden. Ist ein Finanzintermediär laut Spezialgesetz beispielsweise nicht dazu verpflichtet, eine interne Revision einzurichten, so sind die entsprechenden Vorgaben betreffend die interne Revision nicht verpflichtend umzusetzen.
5. Informationshalber wird zur konkreten Umsetzung eines Informationssicherheit-Managementsystems (ISMS) und eines Risikomanagementsystems durch Finanzintermediäre auf folgende internationale Standards verwiesen, ohne diese jedoch für die Finanzintermediäre als verbindlich zu erklären:

    - ISMS: ISO 27001, NIST Cybersecurity Framework, COBIT, BSI Grundschutz
    - Risikomanagementsystem: NIST SP 800-53, ISO 27005

2. Definitionen

Informations- und Kommunikationstechnologien (IKT)

Der Begriff Informations- und Kommunikationstechnologien (IKT) umfasst alle technischen Medien die für die Handhabung von Informationen und zur Unterstützung der Kommunikation eingesetzt werden. Hierzu zählen unter anderem Computer- und Netzwerkhardware sowie die zugehörige Software.

IKT- und Sicherheitsrisiken (inklusive Cyber Risiken)

Verlustrisiko aufgrund einer Verletzung der Vertraulichkeit, Verlust der Integrität von Systemen und Daten, einer unzureichenden oder fehlenden Verfügbarkeit von Systemen und Daten, einer mangelnden Fähigkeit, die Informationstechnologie (IT) in einem angemessenen Zeit- und Kostenrahmen zu ändern, wenn sich die Umgebungs- oder Geschäftsanforderungen ändern (d. h. Agilität). Dies umfasst Sicherheitsrisiken, die aus unzulänglichen oder fehlgeschlagenen internen Prozessen oder externen Ereignissen resultieren, einschliesslich Cyber-Attacken oder unzureichender physischer Sicherheit.

IKT-Systeme

IKT-Komponenten als Teil eines Verbunds oder eines verbundenen Netzwerks, das die Betriebsaktivitäten eines Finanzinstituts unterstützt.

[1] Vgl. bspw. Art. 7a des BankG
[2] https://www.fma-li.li/de/regulierung/regulierungen-der-europaischen-aufsichtsbehorden.html

IKT-Dienste

Dienste, die von IKT-Systemen für einen oder mehrere interne oder externe Nutzer erbracht werden. Beispiele dafür sind Dienste in den Bereichen Datenerfassung, Datenspeicherung, Datenverarbeitung und Berichterstattung, aber auch Überwachungs- sowie Geschäfts- und Entscheidungsunterstützungsdienstleistungen.

IKT-Assets

Der Bestand aus Software und Hardware, die ein Finanzintermediär nutzt, um seine IKT Dienste im Unternehmensumfeld zu erbringen.

IKT-Projekte

Jedes Projekt oder ein Teil davon, bei dem die IKT-Systeme und -Dienste geändert, ersetzt, verworfen oder implementiert werden. IKT-Projekte können Teil eines grösseren IKT- oder Geschäftstransformationsprogramms sein.

IKT-Betriebs- oder IKT-Sicherheitsvorfall

Ein einzelnes Ereignis oder eine Reihe zusammenhängender Ereignisse, die vom Finanzintermediär nicht geplant wurden und sich negativ auf die Integrität, Verfügbarkeit, Vertraulichkeit und/oder Authentizität von IKT-Diensten auswirken oder auswirken könnten.

Leitungsorgan

Das Organ oder die Organe eines Instituts, das (die) bestellt wurde (wurden) und befugt ist (sind), Strategie, Ziele und Gesamtpolitik des Instituts festzulegen und die Entscheidungen der Geschäftsleitung zu kontrollieren und zu überwachen, und dem die Personen angehören, die die Geschäfte des Instituts tatsächlich führen.

Patch

Ein Patch (vom englischen „patch“, auf Deutsch: Flicken) ist ein kleines Programm, das Softwarefehler wie z. B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen behebt.

Penetrationstests / Red-Team-Übungen / Threat-Led-Penetration-Tests

Ein Penetrationstest ist ein gezielter, in der Regel simulierter, Angriffsversuch auf ein IT-System. Er wird als Wirksamkeitsprüfung vorhandener Sicherheitsmassnahmen eingesetzt.

Bei Red-Team-Übungen handelt es sich um die Simulation eines Angriffs auf eine befreundete Infrastruktur durch eine Gruppe (Red Team) unter realistischen Bedingungen, mit dem Ziel der Überprüfung der Sicherheits- und Abwehrmechanismen. Eine andere Gruppe im inneren der Infrastruktur (Blue Team) versucht auf der anderen Seite die Eindringlinge abzuwehren.

Der Threat-Led-Penetration-Test ist ein kontrollierter Versuch, die Cyber-Resilienz eines Unternehmens zu gefährden, indem die Taktiken, Techniken und Verfahren realer Bedrohungsakteure simuliert werden. Es basiert auf gezielten Bedrohungsinformationen und konzentriert sich auf die Mitarbeiter, Prozesse und Technologien eines Unternehmens mit minimalen Vorkenntnissen und Auswirkungen auf den Betrieb.

IKT-Systemlandschaft

IKT-Systemlandschaft beschreibt die Gesamtheit der in einer IKT-Umgebung verwendeten IT- und Kommunikations-Systeme einschliesslich der Anwendungen, sowie sämtliche Infrastrukturkomponenten eines Netzwerkes, die zu verwaltenden elektronischen Daten und die Schnittstellen zwischen den Komponenten.

Wichtige IKT-Dienste und/oder IKT-Systeme (im Kontext von Auslagerungen)

IKT-Dienste und/oder IKT-Systeme, welche gemäss den jeweils für Finanzintermediäre geltende aufsichtsrechtlichen und gesetzlichen Vorgaben kritisch oder wesentlich sind. Falls keine weitergehenden aufsichtsrechtlichen und gesetzlichen Vorgaben für Finanzintermediäre die Wichtigkeit definieren, sind IKT-Dienste und/oder IKT-Systeme die ausgelagert werden wichtig, wenn sie gemäss einer eigenverantwortlichen Einschätzung der Finanzintermediäre für die Erbringung ihrer Dienstleistungen kritisch oder wesentlich sind.

3. IKT-Strategie

6. Das Leitungsorgan eines Finanzintermediärs ist verantwortlich für die Festsetzung, Genehmigung und laufende Überwachung der Umsetzung der IKT-Strategie als Teil ihrer gesamten Unternehmensstrategie sowie für die Schaffung eines wirksamen Risikomanagementrahmens für die IKT- und Sicherheitsrisiken. Finanzintermediäre haben dabei geeignete Verfahren zur Überwachung und Messung der Wirksamkeit der Umsetzung ihrer IKT-Strategie einzuführen. Die IKT-Strategie wird regelmässig sowie anlassbezogen durch das Leitungsorgan auf Aktualität überprüft und gegebenenfalls angepasst.

7. Die IKT-Strategie ist mit der gesamthaften Geschäftsstrategie abgestimmt und konkretisiert die Entwicklung der IKT-Architektur mit einem Überblick über die IKT Systemlandschaft, einschliesslich Abhängigkeiten von Dritten. Die IKT-Strategie beinhaltet mindestens folgende Punkte:

   a) Wie sich die IKT des Finanzintermediärs entwickeln sollte, um die Unternehmensstrategie, einschliesslich der Entwicklung der Organisationsstruktur, der IKT-Systemänderungen (neue Systeme [eigen- und fremdentwickelt] und Änderungen von bestehenden Systemen) und wichtiger Abhängigkeiten von Dritten, effektiv umzusetzen und zu unterstützen.
   b) Ob Auslagerungen für IKT-Dienste und/oder IKT-Systeme angestrebt werden und wenn ja, in welchem Umfang und unter Berücksichtigung welcher Aspekte.
   c) Klare und messbare Ziele betreffend die Informationssicherheit, mit Fokus auf IKT-Systeme und IKT-Dienste, -Personal und -Prozesse.

8. Finanzintermediäre stellen dazu Massnahmenpläne zur Erreichung der Ziele der IKT-Strategie auf. Diese Massnahmen werden allen relevanten Mitarbeitern, einschliesslich Auftragnehmern und Drittanbietern (sofern zutreffend und relevant) kommuniziert und regelmässig überprüft, um ihre Relevanz und Angemessenheit sicherzustellen. Für ausgelagerte IKT Dienste und/oder IKT-Systeme werden die relevanten Massnahmen als Bestandteil der Auslagerung an den Dienstleister delegiert und festgelegt, wie die Erreichung der Ziele durch den Finanzintermediär überwacht wird.

4. IKT-Governance

9. Die IKT-Governance des Finanzintermediärs stellt sicher, dass die IKT-Strategie messbar und wirksam umgesetzt wird. Das Leitungsorgan stellt sicher, dass der Finanzintermediär über eine angemessene interne Governancestruktur und einen angemessenen internen Kontrollrahmen für die IKT- und Sicherheitsrisiken verfügt, der auch ausgelagerte IKT-Dienste und/oder IKT-Systeme umfasst. Das Leitungsorgan legt dabei klare Aufgaben und Verantwortlichkeiten für IKT-Funktionen, Informationsicherheitssrisikomanagement und Business Continuity, einschliesslich derjenigen für das Leitungsorgan und seine Ausschüsse fest.

10. Das Leitungsorgan stellt sicher, dass das Personal des Finanzintermediärs fachlich ausreichend qualifiziert ist und ausreichend Ressourcen zur Verfügung stehen, um die IKT-Betriebsbedürfnisse und die IKT- und Sicherheitsrisikomanagementprozesse fortlaufend zu unterstützen und um die Umsetzung ihrer IKT-Strategie zu gewährleisten. Das Leitungsorgan stellt zudem sicher, dass das zugewiesene Budget zur Erfüllung der oben genannten Anforderungen angemessen ist. Darüber hinaus stellen Finanzintermediäre sicher, dass alle Mitarbeiter, einschliesslich Inhaber von Schlüsselfunktion, angemessene Schulungen zu IKT- und Sicherheitsrisiken, einschliesslich Informationssicherheit, zumindest auf jährlicher Basis erhalten.

11. Die interne Revision des Finanzintermediärs berücksichtigt zudem die IKT- und Sicherheitsrisiken im Rahmen der Prüfungsplanung unter Berücksichtigung der Risikoanalyse in Verbindung mit ihrer Mehrjahresplanung in angemessener Weise.

5. IKT- und Informationssicherheitsrisikomanagement

5.1 Organisation und Ziele

12. Der Finanzintermediär verfügt über ein angemessenes und wirksames IKT- und Informationssicherheitsrisikomanagement-Konzept, welches in das Unternehmens-Risikomanagementkonzept des Finanzintermediärs eingegliedert ist.

13. Finanzintermediäre identifizieren, bewerten und steuern ihre IKT- und Sicherheitsrisiken inklusive derjenigen, die aus Auslagerungen hervorgehen. Die IKT-Funktionen bzw. -Organisationseinheiten, welche für IKT-Systeme, Prozesse und Sicherheitstätigkeiten verantwortlich sind, verfügen über geeignete Prozesse und Kontrollen, um sicherzustellen, dass alle Risiken identifiziert, analysiert, gemessen, überwacht, gesteuert, gemeldet und innerhalb der Grenzen der Risikobereitschaft des Finanzintermediärs gehalten werden können. Zudem entsprechen von ihnen durchgeführte Projekte und bereitgestellte Systeme sowie die durchgeführten Tätigkeiten den externen und internen Anforderungen.

14. Die Finanzintermediäre übertragen die Verantwortung für die Steuerung und Überwachung der IKT- und Sicherheitsrisiken an die Risikomanagementfunktion. Diese stellt sicher, dass IKT- und Sicherheitsrisiken identifiziert, gemessen, bewertet, gesteuert, überwacht und gemeldet werden und ist für die Überwachung und Kontrolle der Einhaltung des IKT-Sicherheitsrisikomanagementrahmenwerks operativ verantwortlich. Finanzintermediäre gewährleisten die Unabhängigkeit und Objektivität der Risikomanagementfunktion, dass eine angemessene Trennung von IKT-Betriebsprozessen sichergestellt ist und stellen zudem sicher, dass die Risikomanagementfunktion nicht für Tätigkeiten der internen Revision verantwortlich ist. Diese Risikomanagementfunktion ist direkt gegenüber der Geschäftsführung rechenschaftspflichtig und für die Überwachung und Kontrolle der Einhaltung des IKT- und Sicherheitsrisikomanagementrahmenwerks verantwortlich.

15. Die interne Revision muss unter Zuhilfenahme eines risikobasierten Ansatzes in der Lage sein, die Übereinstimmung aller IKT- und sicherheitsrelevanten Tätigkeiten und Abteilungen eines Finanzinstituts mit den Grundsätzen und Verfahren des Finanzinstituts und den externen Anforderungen unabhängig zu überprüfen und objektiv zu beurteilen. Finanzintermediäre definieren und weisen wichtige und relevante Rollen, Verantwortlichkeiten und entsprechende Berichtspflichten zu, damit der IKT- und Informationssicherheitsrisikomanagementrahmen wirksam ist.

16. Der Rahmen des IKT- und Informationssicherheitsrisikomanagements umfasst Prozesse, die Folgendes ermöglichen:

    a) Ermittlung der Risikobereitschaft für IKT- und Sicherheitsrisiken in Übereinstimmung mit der Risikobereitschaft des Finanzintermediärs;
    b) Identifikation und Bewertung der IKT- und Sicherheitsrisiken, denen ein Finanzintermediär ausgesetzt ist;
    c) Festlegung von Massnahmen, einschliesslich Kontrollmassnahmen, zur Minderung von IKT- und Sicherheitsrisiken, so dass diese innerhalb der Risikobereitschaft und aufsichtsrechtlichen Anforderungen liegen;
    d) Überwachung der Wirksamkeit dieser Massnahmen sowie Erfassung der Anzahl der gemeldeten Vorfälle, welche Auswirkungen auf IKT-bezogene Aktivitäten haben, und Ergreifen von geeigneten Massnahmen bei Bedarf;
    e) Berichterstattung über die IKT- und Sicherheitsrisiken und Kontrollen gegenüber dem Leitungsorgan;
    f) Identifikation und Beurteilung, ob IKT- und Sicherheitsrisiken bestehen, die sich aus einer wesentlichen Änderung des IKT-Systems oder der IKT-Dienste, -Prozesse oder -Verfahren und/oder nach einem wesentlichen Betriebs- oder Sicherheitsvorfall ergeben.

17. Finanzintermediäre stellen sicher, dass der Rahmen für das IKT- und Informationssicherheitsrisikomanagement eingehalten, dokumentiert und kontinuierlich verbessert wird, basierend auf den während der Implementierung und Überwachung gewonnenen Erkenntnissen. Der Rahmen für das IKT- und Informationssicherheitsrisikomanagement wird mindestens einmal jährlich vom Leitungsorgan überprüft und genehmigt.

5.2 Ermittlung von Funktionen, Prozessen und IKT-Assets

18. Die Finanzintermediäre erstellen eine aktualisierte Übersicht über ihre geschäftlichen Funktionen, Aufgaben, Geschäfts- und Unterstützungsprozesse und halten diese auf dem neuesten Stand, um die Bedeutung ihrer gegenseitigen Abhängigkeiten im Zusammenhang mit IKT- und Sicherheitsrisiken zu ermitteln.

19. Darüber hinaus erstellen die Finanzintermediäre ein Inventar von IKT-Assets, welches ihre Geschäftsfunktionen und Unterstützungsprozesse, wie zum Beispiel IKT-Systeme sowie Abhängigkeiten von anderen internen und externen Systemen abbildet und halten dieses auf dem aktuellen Stand. Im Weiteren führt der Finanzintermediär aktuelle Listen von Mitarbeiter, Auftragnehmer und Dritten und hält diese auf dem neuesten Stand, um in der Lage zu sein, zumindest die IKT-Assets zu verwalten, welche die kritischen Funktionen und Prozesse unterstützen.

5.3 Einstufung der Kritikalität und Risikobewertung

20. Finanzintermediäre stufen die identifizierten Geschäftsfunktionen, Unterstützungsprozesse und IKT-Assets unter 5.2 (Ermittlung von Funktionen, Prozessen und IKT-Assets) in Bezug auf die Kritikalität ein.

21. Um die Kritikalität dieser identifizierten Geschäftsfunktionen, Unterstützungsprozesse und IKT-Assets zu bewerten, berücksichtigen Finanzintermediäre zumindest die Vertraulichkeits-, Integritäts- und Verfügbarkeitsanforderungen. Es gibt klar zugeordnete Zuständigkeiten und Verantwortungen für die IKT-Assets.

22. Wenn die Risikobewertung durchgeführt wird, überprüfen Finanzintermediäre die Angemessenheit der Einstufung der Kritikalität der IKT-Assets sowie die entsprechende Dokumentation.

23. Finanzintermediäre identifizieren die IKT- und Sicherheitsrisiken, welche auf die identifizierten Geschäftsfunktionen, Unterstützungsprozesse und IKT-Assets Einfluss haben, entsprechend der Kritikalität. Diese Risikobewertung wird jährlich oder, falls notwendig, in kürzeren Intervallen durchgeführt und dokumentiert. Solche Risikobewertungen werden auch für alle wesentlichen Änderungen von Infrastruktur, Prozessen oder Verfahren, welche die Geschäftsfunktionen, Unterstützungsprozesse oder IKT-Assets betreffen, durchgeführt und folglich wird die Risikobewertung des Finanzintermediärs aktualisiert.
24. Finanzintermediäre stellen sicher, dass Bedrohungen und Schwachstellen, welche für Geschäftsfunktionen, Unterstützungsprozesse oder IKT-Assets relevant sind, kontinuierlich überwacht werden und überprüfen Risikoszenarien, welche diese beeinflussen, regelmässig.

5.4 Risikominderung

25. Auf Basis der Risikobewertungen ermitteln Finanzintermediäre, welche Massnahmen erforderlich sind, um identifizierte IKT- und Sicherheitsrisiken auf ein akzeptables Mass zu begrenzen und ob Änderungen für bestehende Geschäftsprozesse, Kontrollmassnahmen, IKT-Systeme und IKT-Dienste notwendig sind. Der Finanzintermediär berücksichtigt die Umsetzungsdauer, die erforderlich ist, um diese Änderungen umzusetzen und angemessene Zwischenmassnahmen zu ergreifen, um folglich IKT- und Sicherheitsrisiken zu verringern und innerhalb der IKT- und Sicherheitsrisikobereitschaft des Finanzintermediärs zu bleiben.
26. Die Finanzintermediäre legen Massnahmen fest und setzen diese um, um identifizierte IKT- und Sicherheitsrisiken zu verringern und um IKT-Assets gemäss ihrer Klassifizierung gemäss 5.3 (Einstufung der Kritikalität und Risikobewertung) zu schützen.

5.5 Berichterstattung

27. Finanzintermediäre teilen die Ergebnisse der Risikobewertung dem Leitungsorgan klar und rechtzeitig mit.

5.6 Interne Revision

28. Das Leitungsorgan eines Finanzintermediärs genehmigt den Prüfungsplan einschliesslich etwaiger IKT-Prüfungen und wesentlichen Änderungen daran. Der Prüfungsplan und seine Durchführung, einschliesslich der Prüfungshäufigkeit, spiegeln die inhärenten IKT- und Sicherheitsrisiken des Finanzintermediärs unter Berücksichtigung der Proportionalität wider und werden regelmässig aktualisiert.
29. Ein formaler Prozess mit klaren Zuständigkeiten zur Nachverfolgung und Behebung von kritischen IKT-Prüfungsergebnissen muss definiert sein, einschliesslich zeitlichen Vorgaben für die Behebung.

6. Informationssicherheitsmanagement

6.1 Informationssicherheitsleitlinie

30. Finanzintermediäre erarbeiten und dokumentieren eine Informationssicherheitsleitlinie, in der die übergeordneten Grundsätze und Regeln definiert, ausgearbeitet und dokumentiert werden, zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Informationen der Finanzintermediäre und ihrer Kunden. Die Informationssicherheitsleitlinie steht mit den Informationssicherheitszielen des Finanzintermediärs in Einklang und basiert auf Grundlage der relevanten Ergebnisse des Risikobewertungsprozesses. Die Leitlinie wird vom Leitungsorgan genehmigt.

31. Die Leitlinie beinhaltet eine Beschreibung der wichtigsten Rollen und Verantwortlichkeiten des Informationssicherheitsmanagements. Zudem beinhaltet diese die Anforderungen an Mitarbeiter, Dienstleister, Prozesse und Technologie in Bezug auf Informationssicherheit. Die Leitlinie gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit von kritischen logischen und physischen IKT-Assets, Ressourcen und sensiblen gespeicherten Daten (Data-at-Rest), sowie von sensiblen Daten während der Übertragung (Data-in-Transit) eines Finanzintermediärs. Die Informationssicherheitsleitlinie wird allen Mitarbeitern und relevanten Personen von Auftragnehmern des Finanzintermediärs bei wichtigen IKT-Auslagerungen mitgeteilt, es sei denn, die relevanten Informationen betreffend die Informationssicherheit werden dem Auftragnehmer in der Auslagerungsleitlinie ausreichend mitgeteilt.

6.2 Überwachung der IKT- und Informationssicherheit

32. Finanzintermediäre legen Regelungen und Verfahren fest und setzen diese um, um anomale Aktivitäten, die sich auf die Informationssicherheit von Finanzintermediären auswirken können festzustellen, und um auf diese Ereignisse angemessen reagieren zu können. Im Rahmen dieser kontinuierlichen Überwachung implementieren Finanzintermediäre angemessene und wirksame Massnahmen zur Erkennung und Meldung von physischem Eindringen, Hackerangriffen, unautorisierten Datenabflüssen sowie Verstössen gegen Vertraulichkeit, Integrität und Verfügbarkeit der IKT-Assets. Die kontinuierlichen Überwachungs- und Erkennungsprozesse umfassen Folgendes:

    a) relevante interne und externe Faktoren, einschliesslich Geschäfts- und IKT-Administrationsfunktionen;
    b) Transaktionen und Vorgänge, um Missbrauch des Zugriffs durch Dritte oder anderer Entitäten und internen Missbrauch des Zugangs festzustellen;
    c) potenzielle interne und externe Bedrohungen.

33. Finanzintermediäre etablieren und setzen Prozesse und Organisationsstrukturen um, um Sicherheitsbedrohungen, die sich wesentlich auf ihre Fähigkeit zur Erbringung von Dienstleistungen auswirken können, identifizieren und laufend überwachen zu können. Finanzintermediäre gewährleisten die Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyber-Attacken, insbesondere in Bezug auf kritische und/oder sensitive Daten und IKT-Systeme. Finanzintermediäre verfolgen die technologischen Entwicklungen aktiv, um sicherzustellen, dass sie sich der Sicherheitsrisiken bewusst sind. Finanzintermediäre richten Massnahmen zur Erkennung ein, um beispielsweise mögliche Datenlecks, schädlichen Code und andere Sicherheitsbedrohungen und öffentlich bekannte Sicherheitslücken in Software und Hardware zu identifizieren und ermitteln entsprechende neue Sicherheitsupdates (siehe 8.1 Sicherheit des IKT-Betriebs).

34. Der Sicherheitsüberwachungsprozess hilft einem Finanzintermediär, die Art der Betriebs- oder Sicherheitsvorfälle zu verstehen, um Trends zu identifizieren und die Untersuchungen zu unterstützen.

6.3 Überprüfung, Bewertung und Testing der Informationssicherheit

35. Finanzintermediäre führen Überprüfungen, Bewertungen und Testings von IKT-Systemen, IKT-Diensten und Informationssicherheitsmassnahmen durch, um eine wirksame Identifizierung von Sicherheitsverletzungen, Sicherheitsvorfällen sowie Schwachstellen in ihren IKT-Systemen und IKT-Diensten (siehe 8.1 Sicherheit des IKT-Betriebs) zu gewährleisten. Mittels Good-Practice-Ansätze wie Schwachstellenmanagement mit regelmässigen Verwundbarkeitsanalysen, Penetrationstests, Red-Team-Übungen und weiteren geeigneten Massnahmen überprüfen Finanzintermediäre Sicherheitslücken und schützen somit sensitive Daten und IKT-Systeme.

36. Finanzintermediäre richten ein Rahmenwerk für Informationssicherheitstest ein und setzen dieses um, welches die Robustheit und Wirksamkeit ihrer Massnahmen betreffend Informationssicherheit bewertet und sicherstellt, dass dieses Rahmenwerk die Bedrohungen und Schwachstellen berücksichtigt, welche durch die Bedrohungsüberwachung und den Informationsrisikomanagementprozess identifiziert wurden.

37. Das Rahmenwerk für Informationssicherheitstests stellt sicher, dass Tests:

    a) von unabhängigen Prüfern mit ausreichenden Kenntnissen, Fähigkeiten und Kompetenzen beim Testen von Informationssicherheitsmassnahmen durchgeführt werden, welche nicht an der Entwicklung der Informationssicherheitsmassnahmen beteiligt sind;
    b) umfassende Schwachstellen- und Penetrationstests (einschliesslich Threat-Led-Penetration-Tests wo notwendig und angemessen) beinhalten, die dem ermittelten Risikoniveau der Geschäftsprozesse und Systeme entsprechen.

38. Finanzintermediäre führen laufende und wiederholte Tests der Sicherheitsmassnahmen durch. Für alle kritischen IKT-Systeme werden diese Tests mindestens einmal jährlich durchgeführt. Unkritische Systeme werden regelmässig, mindestens jedoch alle fünf Jahre, anhand eines risikobasierten Ansatzes getestet.

39. Finanzintermediäre stellen sicher, dass Tests der Sicherheitsmassnahmen im Falle von Änderungen an Infrastruktur, Prozessen oder Abläufen und von Änderungen aufgrund von grossen Betriebs- und Sicherheitsvorfällen oder aufgrund der Freigabe neuer oder erheblich veränderter mit dem Internet verbundenen kritischen Anwendungen zeitnah durchgeführt werden.

40. Finanzintermediäre überwachen und bewerten die Ergebnisse der Sicherheitstests, passen Sicherheitsmassnahmen entsprechend an und aktualisieren ihre Sicherheitsmassnahmen bei kritischen IKT-Systemen entsprechend unverzüglich.

41. Aufgrund der beobachteten Sicherheitsbedrohungen und der vorgenommenen Änderungen werden Tests mit Einbindung von Szenarien relevanter und bekannter potenzieller Angriffe durchgeführt.

6.4 Schulung und Sensibilisierung für Informationssicherheit

42. Finanzintermediäre richten ein Schulungsprogramm einschliesslich der regelmässigen Sicherheit-Sensibilisierungsprogramme für alle Mitarbeiter und für relevante Personen ein, um sicherzustellen, dass sie für die Ausführung ihre Pflichten und Verantwortlichkeiten im Einklang mit den einschlägigen Informationsicherheitsleitlinien und -verfahren geschult sind, um menschliche Fehler, Diebstahl, Betrug, Missbrauch oder Verlust zu verringern und diese geschult werden, wie Informationssicherheitsrisiken entsprechend angegangen werden können. Finanzintermediäre stellen sicher, dass Schulungen für alle Mitarbeiter und für relevante Personen mindestens jährlich durchgeführt werden. Schulungen können durch Mitarbeiter oder durch assoziierte oder externe Fachspezialisten durchgeführt werden.

7. Benutzerberechtigungsmanagement

7.1 Logische Sicherheit / Zugriffsschutz

43. Finanzintermediäre definieren, dokumentieren und implementieren Verfahren für logische Zugriffskontrollen (Identitäts- und Zugriffsverwaltung). Diese Verfahren werden umgesetzt, durchgesetzt, überwacht und regelmässig überprüft. Die Verfahren schliessen auch Kontrollen zur Überwachung von Anomalien ein. Diese Verfahren implementieren mindestens folgende Elemente, bei denen der Begriff „Benutzer" auch technische Benutzer umfasst:

    a) Need-to-Know, Least-Privilege und Funktionstrennung: Finanzintermediäre verwalten Zugriffsrechte auf IKT-Assets und ihre unterstützenden Systeme, auch für Fernzugriffe, auf einer Need-to-Know-Basis. Benutzern wird ein Mindestmass an Zugriffsrechten gewährt, dass zur Erfüllung ihrer Pflichten unbedingt erforderlich ist (Least-Privilege-Prinzip), das heisst um ungerechtfertigten Zugang zu einer grossen Menge von Daten zu verhindern oder die Zuweisung von Kombinationen von Zugriffsrechten, mit denen Kontrollmechanismen umgangen werden können, zu verhindern (Grundsatz der Funktionstrennung).
    b) Rechenschaftspflicht der Nutzer: Finanzintermediäre schränken die Verwendung von generische und gemeinsam genutzte Benutzerkonten so weit wie möglich ein und stellen sicher, dass Benutzer für durchgeführte Aktionen in den IKT-Systemen identifiziert werden können.
    c) Privilegierte Zugriffsrechte: Finanzintermediäre gewährleisten strenge Kontrollen von privilegierten Systemzugriffen durch strikte Beschränkung und Überwachung der Konten mit erhöhten Systemzugriffsrechten (z.B. Administratorkonten). Um eine sichere Kommunikation und Risikominimierung zu gewährleisten, wird administrativer Fernzugriff auf wichtige IKT-Systeme nur auf Need-to-Know-Basis und unter Verwendung von starken Authentifizierungslösungen verwendet.
    d) Protokollierung von Benutzeraktivitäten: Alle Aktivitäten durch privilegierte Benutzer werden protokolliert und überwacht. Zugriffsprotokolle werden für einen angemessenen Zeitraum entsprechend der Kritikalität der identifizierten Geschäftsfunktionen, Unterstützungsprozesse und IKT-Assets, gemäss 5.3 (Einstufung der Kritikalität und Risikobewertung), unbeschadet der Aufbewahrungspflichten im EU- und nationalen Recht aufbewahrt. Der angemessene Zeitraum richtet sich nach den generellen Aufbewahrungsfristen gemäss Personen- und Gesellschaftsrecht (PGR). Ein Finanzintermediär nutzt diese Informationen, um die Identifizierung und Untersuchung von anomalen Aktivitäten aus der Erbringung von Diensten zu fördern.
    e) Zugriffsverwaltung: Zugriffsrechte werden nach vordefinierten Freigabe-Workflows, welche den Eigentümer der Informationen involvieren, zeitnah (unmittelbar nach Eintritt/Kenntnis eines Ereignisses) erteilt, entzogen oder geändert. Im Falle einer Kündigung des Beschäftigungsverhältnisses werden die Zugangsrechte unverzüglich entzogen.
    f) Zugangsrezertifizierung: Die Zugangsrechte werden regelmässig überprüft, um sicherzustellen, dass die Benutzer keine übermässigen Privilegien besitzen und dass Zugriffsrechte entzogen werden, wenn diese nicht mehr erforderlich sind.
    g) Authentifizierungsmethoden: Finanzintermediäre setzen Authentifizierungsmethoden durch, die ausreichend robust sind, um angemessene und effektive Zugriffskontrollen gemäss den Regelungen und Verfahren zu gewährleisten. Authentifizierungsmethoden sind der Kritikalität von IKT-Systemen, IKT-Informationen oder des jeweiligen Zugriffprozesses angemessen. Dies umfasst mindestens komplexe Passwörter oder starke Authentifizierungsmethoden (z.B. Zwei-Faktor-Authentifizierung), basierend auf dem relevanten Risiko.

44. Der elektronische Zugriff von Anwendungen auf Daten und IKT-Systeme wird auf ein Minimum beschränkt, welches notwendig ist, um die entsprechende Dienstleistung zu erbringen.

7.2 Physische Sicherheit

45. Die physischen Sicherheitsmassnahmen der Finanzintermediäre werden definiert, dokumentiert und implementiert, um ihre Räumlichkeiten, Rechenzentren und sensiblen Bereiche vor unbefugtem Zugang und vor Umweltgefahren zu schützen.

46. Der physische Zugang zu IKT-Systemen wird nur befugten Personen gestattet. Genehmigungen werden in Übereinstimmung mit den Aufgaben und Verantwortlichkeiten des Einzelnen zugewiesen und auf Personen beschränkt, die entsprechend geschult und überwacht werden. Der physische Zugang wird regelmässig überprüft, um sicherzustellen, dass unnötige Zugriffsrechte unverzüglich widerrufen werden, wenn sie nicht benötigt werden.

47. Angemessene Massnahmen zum Schutz vor Umweltgefahren entsprechen der Wichtigkeit der Gebäude und der Kritikalität der in diesen Gebäuden befindlichen Tätigkeiten oder IKT-Systemen.

8. IKT-Betriebsmanagement

48. Finanzintermediäre steuern ihre IKT-Tätigkeiten auf der Grundlage von dokumentierten und implementierten Prozessen und Verfahren, die vom Leitungsorgan festgelegt wurden. Diese Dokumente legen fest, wie Finanzintermediäre ihre IKT- Systeme und -Dienste, einschliesslich der Dokumentation kritischer IKT-Vorgänge, betreiben, überwachen und kontrollieren, und ermöglicht Finanzintermediären, ein aktuelles IKT-Systeminventar zu führen.

49. Finanzintermediäre stellen sicher, dass die Leistung ihrer IKT-Tätigkeiten an ihre Geschäftsanforderungen ausgerichtet ist. Finanzintermediäre verbessern und halten, wenn möglich, die Effizienz ihrer IKT-Tätigkeiten aufrecht, einschliesslich aber nicht limitiert auf die Notwendigkeit der Minimierung von potenziellen Fehlern, welche durch die Ausführung manueller Tätigkeiten entstehen.

50. Finanzintermediäre implementieren Protokollierungs- und Überwachungsverfahren für die kritischen IKT-Tätigkeiten zur Erkennung, Analyse und Korrektur von Fehlern.

51. Die Finanzintermediäre führen ein aktuelles Verzeichnis ihrer IKT-Assets (einschließlich IKT-Systeme, Netzwerkgeräte, Datenbanken usw.). Das IKT-Systeminventar enthält die Konfiguration der IKT-Systeme sowie die Verbindungen und Abhängigkeiten zwischen den verschiedenen IKT-Systemen, um einen ordnungsgemässen Konfigurations- und Änderungsmanagementprozess zu ermöglichen.

52. Das IKT-Systeminventar ist ausreichend detailliert, dass eine sofortige Identifizierung eines Systems, seines Standorts, Sicherheitsklassifizierung und Eigentümerschaft möglich ist. Interdependenzen zwischen Systemen werden dokumentiert, um bei der Reaktion auf Sicherheits- und Betriebsstörungen, einschliesslich Cyber-Angriffen, zu unterstützen. Es sind wirksame Prozesse für die Beschaffung und Entsorgung von IKT-Assets einzurichten, um die Bestandesaufnahme zeitnah und lückenlos zu aktualisieren.

53. Finanzintermediäre überwachen und verwalten den Lebenszyklus von IKT-Systemen, um sicherzustellen, dass diese weiterhin die Anforderungen des Geschäfts- und Risikomanagements erfüllen und unterstützen. Finanzintermediäre überwachen, ob ihre IKT-Systeme von ihren externen oder internen Anbietern und Entwicklern unterstützt werden und ob alle relevanten Patches und Upgrades, basierend auf dokumentierten Prozessen, durchgeführt werden. Risiken, die sich aus veralteten oder nicht unterstützten IKT-Systemen ergeben, werden bewertet und abgeschwächt.

54. Finanzintermediäre implementieren Prozesse zur Leistungs- und Kapazitätsplanung sowie der Leistungsüberwachung, um auf wichtige Leistungsprobleme von IKT-Systemen und IKT-Kapazitätsengpässe rechtzeitig zu reagieren, diese zu erkennen und zu vermeiden.

55. Finanzintermediäre definieren und implementieren Sicherung- und Wiederherstellungsverfahren für Daten und IKT-Systeme, um sicherzustellen, dass diese bei Bedarf wiederhergestellt werden können. Der Umfang und die Häufigkeit von Sicherungen steht im Einklang mit den Anforderungen an die Geschäftswiederherstellung sowie der Kritikalität der Daten und der IKT-Systeme und wird anhand der durchgeführten Risikobewertung beurteilt. Das Testen der Sicherungs- und Wiederherstellungsverfahren erfolgt periodisch.

56. Finanzintermediäre stellen sicher, dass Daten- und IKT-Systemsicherungen sicher gespeichert werden und ausreichend weit vom Primärstandort entfernt sind, sodass diese nicht denselben umgebungsbezogenen Risiken ausgesetzt sind.

8.1 Sicherheit des IKT-Betriebs

57. Finanzintermediäre implementieren Verfahren, um das Auftreten von Sicherheitsproblemen in IKT-Systemen und IKT-Diensten zu verhindern, deren Auswirkungen auf die Bereitstellung von IKT-Diensten zu minimieren sowie die Steuerung der Infrastruktur- und Netzwerksicherheit sicherzustellen. Diese Verfahren haben folgende Massnahmen zu umfassen:

    a) Ermittlung potenzieller Schwachstellen, welche bewertet und behoben werden, indem sichergestellt wird, dass Software und Firmware (einschliesslich der von Finanzintermediären an ihre internen und externen Benutzer bereitgestellten Software), wo verfügbar, durch die Bereitstellung kritischer Sicherheits-Patches auf dem neuesten Stand sind oder durch Implementierung von alternativen Massnahmen ausreichend geschützt sind;
    b) Definition, Implementierung und regelmässige Überwachung sicherer Basiskonfiguration aller Netzwerkkomponenten;
    c) Implementierung einer Netzwerksegmentierung, eines Systems zur Verhinderung von Datenverlust und einer Verschlüsselung des Netzwerkverkehrs ausserhalb geschützter Netzwerkzonen (Data-in-transit) (gemäss der Datenklassifizierung);
    d) Implementierung des Schutzes von Endpunkten, einschliesslich Servern, Arbeitsplätzen und Mobilgeräten; Finanzintermediäre bewerten, ob Endpunkte die Sicherheitsanforderungen der von ihnen festgelegte Sicherheitsstandards erfüllen, bevor ihnen Zugriff auf das Unternehmensnetzwerk gewährt wird;
    e) Sicherstellung, dass Mechanismen vorhanden sind, um die Integrität von Software, Firmware und Daten zu überprüfen (insbesondere sicherheitsrelevante Einstellungen);

58. Darüber hinaus stellen die Finanzintermediäre fortlaufend fest, ob Änderungen des vorhandene Betriebsumfelds die vorhandenen Sicherheitsmassnahmen beeinflussen oder ob diese die Ergreifung zusätzlicher Massnahmen zur angemessenen Minderung der damit verbundenen Risiken erfordern. Diese Änderungen sind Teil des formellen Änderungsmanagementprozesses der Finanzintermediäre, der sicherstellt, dass Änderungen ordnungsgemäss geplant, getestet, dokumentiert, autorisiert und bereitgestellt werden.

8.2 Management von IKT-Vorfällen und -Problemen

59. Finanzintermediäre implementieren und richten einen Vorfalls- und Problem-Managementprozess ein, welcher zur Überwachung und Protokollierung betrieblicher und sicherheitsrelevanter IKT-Vorfälle dient und welcher es Finanzintermediären ermöglicht, wichtige Geschäftsfunktionen und Prozesse zeitnah gemäss 11. (Notfallkonzept und Business Continuity Management) fortzusetzen oder wieder aufzunehmen, wenn Störungen auftreten. Finanzintermediäre legen geeignete Kriterien und Schwellenwerte für die Klassifizierung von Ereignissen als Betriebs- oder Sicherheitsvorfälle, sowie Frühwarnindikatoren, die als Warnungen zur frühzeitigen Erkennung dieser Vorfälle dienen, fest.

60. Um die Auswirkungen von unerwünschten Ereignissen zu minimieren und eine rechtzeitige Wiederherstellung zu ermöglichen, haben die Finanzintermediäre geeignete Prozesse und Organisationsstrukturen festzulegen, um eine kohärente und integrierte Überwachung, Behandlung und Nachverfolgung von Betriebs- und Sicherheitsvorfällen sicherzustellen und, dass die Hauptursachen identifiziert und beseitigt werden, um das Auftreten von wiederholten Vorfällen verhindern. Der Vorfalls- und Problem-Managementprozess legt Folgendes fest:

    a) die Verfahren zur Identifizierung, Verfolgung, Protokollierung, Kategorisierung und Klassifizierung von Vorfällen gemäss einer Priorisierung, basierend auf der Geschäftskritikalität;
    b) die Rollen und Verantwortlichkeiten für verschiedene Vorfallszenarien (z.B. Fehler, Funktionsstörungen, Cyber-Angriffe);
    c) Problemmanagementverfahren zur Identifizierung, Analyse und Lösung der zugrunde liegenden Ursache eines oder mehrere Vorfälle. Ein Finanzintermediär analysiert Betriebs- oder Sicherheitsvorfälle, von denen der Finanzintermediär wahrscheinlich betroffen ist, welche identifiziert wurden oder innerhalb und/oder ausserhalb der Organisation aufgetreten sind und berücksichtigt wichtige gewonnene Erkenntnisse aus diesen Analysen und aktualisiert die Sicherheitsmassnahmen entsprechend;
    d) wirksame interne Kommunikationspläne, einschliesslich Meldung von Vorfällen und Eskalationsverfahren, die auch sicherheitsrelevante Kundenbeschwerden abdecken, um sicherzustellen, dass:
        i. Vorfälle mit potenziell hohen nachteiligen Auswirkungen auf kritische IKT-Systeme und IKT-Dienste an die Leitungsebene der IKT-Abteilung und an das für IKT verantwortliche Leitungsorgan gemeldet werden;
        ii. das Leitungsorgan ad hoc bei schwerwiegenden Zwischenfällen, zumindest über die Auswirkungen, die Reaktion und die zusätzlichen Kontrollen, die aufgrund der Vorfälle definiert werden müssen, informiert wird.
    e) Verfahren zur Reaktion auf Vorfälle, um die mit den Vorfällen verbundenen Auswirkungen abzuschwächen und sicherstellen, dass der Dienst rechtzeitig betriebsbereit und sicher ist;
    f) spezifische externe Kommunikationspläne für kritische Geschäftsfunktionen und -prozesse um:
        i. mit relevanten Stakeholdern, wie z.B. Dienstleistern, zusammenzuarbeiten, um effektiv zu reagieren und die Wiederherstellung nach einem Vorfall zu gewährleisten;
        ii. externe Parteien (z.B. Kunden, andere Marktteilnehmer, Aufsichtsbehörden) gegebenenfalls rechtzeitig im Einklang mit den geltenden Vorschriften zu informieren.

9. IKT-Projekte und Änderungsmanagement

9.1 IKT-Projektmanagement

61. Der Finanzintermediär implementiert ein Programm und/oder einen Projekt-Governance-Prozess, welcher Rollen, Verantwortlichkeiten und Zuständigkeiten definiert, um die Umsetzung der IKT-Strategie effektiv zu unterstützen.

62. Der Finanzintermediär überwacht und mindert die von seinem Portfolio von IKT-Projekten (Programmmanagement) ausgehenden Risiken angemessen, unter Berücksichtigung der Risiken, die sich aus Abhängigkeiten zwischen verschiedenen Projekten und von Abhängigkeiten mehrerer Projekte von den gleichen Ressourcen und/oder Fachkenntnissen ergeben können. Der Finanzintermediär berücksichtigt dabei zudem Projekte, welche wesentliche Änderungen an IKT Systemen zur Folge haben und Projekte, welche wesentliche Auswirkungen auf die Risiken in der IKT-Sicherheit haben.

63. Der Finanzintermediär stellt eine IKT-Projektmanagementrichtlinie auf und setzt diese um, die mindestens Folgendes beinhaltet:

    a) Projektziele;
    b) Rollen und Verantwortlichkeiten;
    c) eine Projektrisikobewertung;
    d) einen Projektplan, einen Zeitrahmen und Projektschritte;
    e) wichtige Meilensteine;
    f) Anforderungen an das Änderungsmanagement;
    g) Abnahmekriterien zur Übergabe neuer IKT Funktionen an den Betrieb.

64. Die IKT-Projektmanagementrichtlinie stellt sicher, dass die Anforderungen an die Informationssicherheit von einer von der Entwicklungsfunktion unabhängigen Funktion analysiert und freigegeben sind.

65. Der Finanzintermediär stellt sicher, dass alle von einem IKT-Projekt betroffenen Bereiche im Projektteam vertreten sind, und dass das Projektteam über die erforderlichen Kenntnisse verfügt (einschliesslich die entsprechenden Funktionen und Kompetenzen aus den verschiedenen IKT-Bereichen basierend auf dem Risiko), um eine sichere und erfolgreiche Projektumsetzung sicherzustellen.

66. Über die Einrichtung und den Fortschritt von IKT-Projekten und die damit verbundenen Risiken wird an das Leitungsorgan einzeln oder zusammenfassend, je nach Bedeutung und Grösse der IKT-Projekte, regelmässig oder ad hoc berichtet. Finanzintermediäre integrieren Projektrisiken in ihr Risikomanagementsystem.

9.2 Erwerb und Entwicklung von IKT-Systemen

67. Die Finanzintermediäre entwickeln und setzen einen Prozess um, der den Erwerb, die Entwicklung und die Wartung von IKT-Systemen regelt. Dieser Prozess wird auf einem risikobasierten Ansatz eingerichtet.

68. Der Finanzintermediär stellt sicher, dass vor dem Erwerb oder der Entwicklung von IKT-Systemen die funktionalen und nicht funktionalen Anforderungen (einschliesslich Anforderungen an die Informationssicherheit) klar definiert und vom jeweiligen Leitungsorgan genehmigt sind.

69. Der Finanzintermediär stellt sicher, dass Massnahmen zur Risikominderung von unbeabsichtigter Veränderung oder absichtlicher Manipulation der IKT-Systeme während der Entwicklung und Implementierung in der Produktionsumgebung getroffen werden.

70. Finanzintermediäre verfügen über eine Methodik zum Testen und Genehmigen von IKT-Systemen vor ihrer ersten Verwendung. Diese Methodik berücksichtigt die Kritikalität des Geschäftsprozesses und der Vermögenswerte. Die Tests stellen sicher, dass neue IKT-Systeme wie vorgesehen funktionieren. Sie verwenden auch Testumgebungen, die die Produktionsumgebung angemessen widerspiegeln.

71. Finanzintermediäre implementieren separate IKT-Umgebungen, um Funktionsstörungen und Auswirkungen nicht verifizierter Änderungen an den Produktionssystemen zu mindern. Insbesondere stellt ein Finanzintermediär die Trennung der Produktionsumgebungen von Entwicklungs-, Test- und anderen Nicht-Produktionsumgebungen sicher. Ein Finanzintermediär gewährleistet die Integrität und Vertraulichkeit der Produktionsdaten in Nicht-Produktionsumgebungen. Der Zugriff auf Produktionsdaten ist auf autorisierte Benutzer beschränkt. Die Daten der Testumgebung unterliegen den gleichen Schutzanforderungen wie die Daten der Produktionsumgebung, sobald Produktivdaten auf der Testumgebung verwendet werden.

72. Finanzintermediäre ergreifen Massnahmen zum Schutz der Integrität der Quellcodes von IKT-Systemen, die im eigenen Haus entwickelt werden. Sie dokumentieren auch die Entwicklung, Implementierung, Betrieb und/oder Konfiguration der IKT-Systeme umfassend, um jede unnötige Abhängigkeit von Fachexperten zu reduzieren. Die Dokumentation des IKT-Systems enthält, wenn anwendbar, mindestens Benutzerdokumentation, technische Systemdokumentation und Arbeitsanweisungen.

73. Die Prozesse eines Finanzintermediärs für den Erwerb und die Entwicklung von IKT-Systemen gelten auch für IKT-Systeme, die von den Endbenutzern der Geschäftsfunktion ausserhalb der IKT-Organisation entwickelt oder verwaltet werden (z.B. Endbenutzer-Computeranwendungen), unter Verwendung eines risikobasierten Ansatzes. Der Finanzintermediär führt ein Verzeichnis der Anwendungen, welche wesentliche Geschäftsfunktionen oder -prozesse unterstützen.

9.3 IKT-Änderungsmanagement

74. Finanzintermediäre richten einen IKT-Änderungsmanagement-Prozess ein und setzen diesen um, um sicherzustellen, dass alle Änderungen an IKT-Systemen – insbesondere auch sicherheitsrelevante Konfigurationsänderungen – in kontrollierter Art und Weise aufgezeichnet, getestet, bewertet, genehmigt, umgesetzt und überprüft werden. Finanzintermediäre gehen mit Änderungen während Notfällen (d.h. Änderungen, die so bald wie möglich eingeführt werden müssen) nach Verfahren, welche angemessene Sicherheitsvorkehrungen bieten, vor.

75. Die Finanzintermediäre stellen fest, ob Änderungen in der bestehenden Betriebsumgebung die bestehenden Sicherheitsmassnahmen beeinflussen oder ob dies neue Massnahmen zur Minderung der damit verbundenen Risiken benötigt. Diese Änderungen sind in Übereinstimmung mit den formalen Änderungsmanagementprozessen der Finanzintermediäre.

10. Auslagerungen (inkl. Cloud)

10.1 Grundsätze

76. Die Auslagerung von IKT-Diensten und/oder IKT-Systemen führt nicht zur Delegation der Verantwortlichkeiten des Finanzintermediärs. Finanzintermediäre bleiben in vollem Masse für die Erfüllung ihrer regulatorischen Pflichten verantwortlich und rechenschaftspflichtig, einschliesslich der Fähigkeit zur Beaufsichtigung der ausgelagerten IKT-Dienste und/oder IKT-Systeme. Gegenüber der FMA tragen Finanzintermediäre die Verantwortung für ausgelagerte IKT-Dienste und/oder IKT-Systeme, wie wenn sie diese selbst betreiben würden.

77. Finanzintermediäre haben für die Auslagerung von IKT-Diensten und/oder IKT-Systemen:

    a. eine eindeutige Zuweisung der Zuständigkeiten für die Dokumentation, das Management und die Kontrolle von Auslagerungsvereinbarungen vorzunehmen:
        i. Finanzintermediäre richten im Rahmen ihrer Risikomanagement-Funktion eine gesonderte Auslagerungsfunktion ein oder benennen – sofern aufgrund der gesetzlichen Grundlagen zulässig – eine Führungskraft. Im zweiten Fall muss die Führungskraft unmittelbar dem Leitungsorgan unterstellt sein (z.B. ein Inhaber einer Schlüsselfunktion hinsichtlich einer Kontrollfunktion). Die Auslagerungsfunktion bzw. die Führungskraft ist für die Steuerung und die Kontrolle der Risiken von Auslagerungsvereinbarungen als Teil des internen Kontrollrahmens des Finanzintermediärs sowie für die Überwachung der Dokumentation von Auslagerungsvereinbarungen verantwortlich;
        ii. Finanzintermediäre können unter Beachtung von Proportionalitätsaspekten die Auslagerungsfunktion einem Mitglied ihrer Geschäftsleitung übertragen. Aufgaben und Zuständigkeit für das Management und die Kontrolle von Auslagerungsvereinbarungen sind klar zu trennen;
    b. ausreichende Mittel zuzuweisen, um die Erfüllung aller rechtlichen und aufsichtlichen Anforderungen einschliesslich der vorliegenden Richtlinie sowie die Dokumentation und Überwachung aller Auslagerungsvereinbarungen zu gewährleisten;
    c. zu definieren, wie sie die Abhängigkeiten von Dienstleistern mittels Risikobewertung, Business Continuity Management und Ausstiegsstrategien auf ein akzeptables Mass reduzieren.

78. Vor dem Abschluss einer Auslagerungsvereinbarung haben Finanzintermediäre:

    a. zu prüfen, ob die Auslagerungsvereinbarung wichtige IKT-Dienste und/oder IKT-Systeme betrifft;
    b. alle relevanten Risiken der Auslagerungsvereinbarung zu ermitteln und zu bewerten;
    c. eine angemessene Due-Diligence-Prüfung des potenziellen Dienstleisters vorzunehmen;
    d. die Erfüllung der für sie geltenden aufsichtsrechtlichen Anforderungen zu bewerten;
    e. Interessenkonflikte, die sich aus der Auslagerung ergeben können, zu ermitteln und zu bewerten.

79. Finanzintermediäre wählen für die Risikobewertung und die Due-Diligence Prüfung einen Ansatz, der in einem angemessenen Verhältnis zu der Art, dem Umfang und der Komplexität der Risiken steht, die mit den an Dienstleister ausgelagerten IKT-Dienste und/oder IKT-Systeme einhergehen.

80. Die interne Revision der Finanzintermediäre überprüft unabhängig und nach einem risikobasierten Ansatz die korrekte und wirksame Umsetzung des Rahmenwerks für Auslagerungen des Finanzintermediärs. Der Prüfplan sollte insbesondere die Auslagerungsvereinbarungen für wichtige IKT-Dienste und/oder IKT-Systeme umfassen.

10.2 Auslagerungsrichtlinien

81. Auslagerungsrichtlinien beschäftigen sich mit der praktischen Umsetzung der Vorgaben der Auslagerungsstrategie. Finanzintermediäre haben über schriftliche Auslagerungsrichtlinien zu verfügen, die von dem Organ genehmigt wurde, das befugt ist, Strategie, Ziele und Gesamtpolitik des Finanzintermediärs festzulegen und die Entscheidungen der Geschäftsleitung zu kontrollieren. Sie überprüfen und aktualisieren die schriftlichen Auslagerungen regelmässig und stellen deren Umsetzung sicher. Die Auslagerungsrichtlinien umfassen die zentralen Phasen des Lebenszyklus von Auslagerungsvereinbarungen und enthalten Definitionen der Grundsätze, Zuständigkeiten, Rollenbezeichnungen, Aufgaben und Prozesse bezüglich Auslagerungen. Sie tragen zudem der Art der Auslagerung (Managed Services, Hosting, Cloud, usw.) Rechnung. Weiter legen Auslagerungsrichtlinien die für die Auswahl und die Zusammenarbeit mit einem Dienstleister massgebenden Kriterien und Faktoren fest. Sie legen auch fest, ob Weiterverlagerungen von ausgelagerten wichtigen IKT-Diensten und/oder Systemen von Dienstleistern an Subunternehmen möglich sind und unter welchen Bedingungen.

10.3 Wichtige IKT-Dienste und/oder IKT-Systeme

82. Vor dem Abschluss einer Auslagerungsvereinbarung mit einem Dienstleister prüfen Finanzintermediäre, ob die Auslagerungsvereinbarung IKT-Dienste und/oder IKT-Systeme betrifft, die wichtig sind. Bei dieser Prüfung ziehen Finanzintermediäre gegebenenfalls in Erwägung, ob die IKT-Dienste und/oder Systeme in Zukunft potenziell wichtig werden könnten. Ferner unterziehen Finanzintermediäre die Wichtigkeit der IKT-Dienste und/oder IKT-Systeme, die bereits an einen Dienstleister ausgelagert wurden, einer neuerlichen Prüfung, wenn sich erhebliche Änderungen der Art, des Umfangs oder der Komplexität der mit der Auslagerungsvereinbarung verbundenen Risiken ergeben.

10.4 Risikobewertung

83. Finanzintermediäre stellen sicher, dass Entscheidungen über die Auslagerung von IKT-Diensten und/oder IKT-Systemen an einen Dienstleister auf der Grundlage einer eingehenden Risikobewertung getroffen werden, bei der auch alle relevanten Risiken berücksichtigt werden, die sich aus der Auslagerungsvereinbarung ergeben. Die IKT- und Sicherheitsrisiken aufgrund von Auslagerungen sind im Rahmen des IKT- und Informationssicherheitsrisikomanagements (siehe auch 5.1 Organisation und Ziele) zu bewerten.

84. Bei der Risikobewertung berücksichtigen Finanzintermediäre die erwarteten Vorteile und Kosten der geplanten Auslagerungsvereinbarung, einschliesslich der Abwägung etwaiger Risiken, die verringert oder besser gesteuert werden können, gegenüber Risiken, die durch die geplante Auslagerungsvereinbarung entstehen können.

85. Finanzintermediäre berücksichtigen bei der Auslagerung wichtiger IKT-Dienste und/oder IKT-Systeme in ihrer Risikobewertung insbesondere Folgendes:

    a) die Ausgestaltung der Auslagerung (z.B. Art der Auslagerung, Dienstleistungsmodell);
    b) den Einfluss auf das Business Continuity Management;
    c) Konzentrationsrisiken, wenn mehrere IKT-Dienste und/oder IKT-Systeme an einen einzigen Dienstleister ausgelagert werden oder wenn ein Dienstleister nicht problemlos ersetzbar ist;
    d) Risiken im Zusammenhang mit dem Migrationsprozess der Daten sowie der IKT-Dienste und/oder IKT Systeme;
    e) Risiken im Zusammenhang mit der Sensitivität der auszulagernden IKT-Dienste und/oder IKT-Systeme, der Sensitivität der dazu gehörenden Daten und die deswegen erforderlichen Sicherheitsmassnahmen;

f) Risiken in Bezug auf Länder, in denen der Dienstleister seine Niederlassung hat, sowie in Bezug auf Länder, in denen die ausgelagerten IKT-Dienste und/oder IKT-Systeme bereitgestellt werden und/oder in denen Daten gespeichert oder verarbeitet werden:
   i. hinsichtlich der politischen Situation und Sicherheitslage;
   ii. hinsichtlich der geltenden Gesetze inkl. Rechtsvorschriften zum Datenschutz;
   iii. hinsichtlich der geltenden Bestimmungen zur Rechtsdurchsetzung;
   iv. hinsichtlich der insolvenzrechtlichen Vorschriften, die beim Ausfall eines Dienstleisters Anwendung fänden, sowie etwaige Einschränkungen, die insbesondere bezüglich der dringenden Wiederherstellung der Daten von Finanzintermediären entstehen könnten;
   v. hinsichtlich Aufsichtsbeschränkungen

g) Mit Weiterverlagerungen verbundene Risiken (inkl. Risiken aufgrund von langen und komplexen Auslagerungsketten).

86. Finanzintermediäre stellen die Umsetzung und Wirksamkeit der in ihrem Risikomanagementrahmen definierten Risikominderungsmassnahmen sicher.

87. Die Risikobewertung wird vor einer Auslagerung durchgeführt und danach regelmässig überprüft. Falls Finanzintermediäre Kenntnis von erheblichen Mängeln und/oder erheblichen Veränderungen bei den erbrachten Dienstleistungen oder der Situation von Dienstleistern erlangen, wird die Risikobewertung umgehend überprüft oder erneut durchgeführt. Bei einer Erneuerung einer Auslagerungsvereinbarung, die den Inhalt und den Umfang dieser Vereinbarung betrifft, (z.B. Erweiterung des Umfangs oder Aufnahme von wichtigen IKT-Diensten und/oder IKT-Systemen, die zuvor nicht inbegriffen waren, in den Vereinbarungsumfang) ist eine Risikobewertung erneut durchzuführen.

10.5 Due-Diligence-Prüfung

88. Finanzintermediäre legen einen Prozess zur Auswahl und Genehmigung von Dienstleistern fest, um sicherzustellen, dass Dienstleister zur Erbringung der geplanten Auslagerung von IKT-Diensten und/oder IKT-Systemen geeignet sind (die Due-Diligence-Prüfung).

89. Finanzintermediäre stellen durch ihre Due-Diligence-Prüfung sicher, dass Dienstleister den Kriterien ihrer schriftlich festgelegten Auslagerungsrichtlinien entsprechen (siehe auch Punkt 10.2 Auslagerungsrichtlinien).

90. Finanzintermediäre stellen bei der Auslagerung wichtiger IKT-Dienste und/oder IKT-System sicher, dass Dienstleister über die geschäftliche Reputation, angemessene und ausreichende Fähigkeiten, Fachkenntnisse, Kapazitäten, Mittel (z. B. personelle und finanzielle Mittel, IT-Ressourcen), Infrastruktur, Organisationsstruktur und gegebenenfalls die erforderliche(n) aufsichtliche(n) Zulassung(en) oder Registrierung(en) zur Wahrnehmung der IKT-Dienste und/oder IKT-Systeme in zuverlässiger und professioneller Weise verfügen, um ihre Verpflichtungen während der Laufzeit der Auslagerungsvereinbarung zu erfüllen. Dienstleister müssen Gewähr für eine sichere und dauerhafte Leistungserbringung bieten und über ein angemessenes IKT-Änderungsmanagement sinngemäss nach Punkt 9. (IKT- Projekte und Änderungsmanagement) verfügen.

91. Wenn die Auslagerung die Verarbeitung personenbezogener oder vertraulicher Daten umfasst, haben sich Finanzintermediäre davon zu überzeugen, dass Dienstleister entweder keinen Zugriff auf die Daten erlangen können (zum Beispiel durch dienstleisterunabhängige Verschlüsselung) oder angemessene technische, personelle und organisatorische Massnahmen zum Schutz der Daten umsetzen. Dies ist insbesondere der Fall, wenn Dienstleister ihre Dienstleistungen mehreren Unternehmen anbieten. Die Vertraulichkeit der Daten muss nicht nur gegenüber Dritten, sondern auch zwischen den verschiedenen auslagernden Unternehmen gewahrt sein.

92. Gegebenenfalls können Finanzintermediäre zur Unterstützung der bei der Due-Diligence-Prüfung gewonnenen Erkenntnisse Zertifizierungen auf der Grundlage von internationalen Standards, Prüfberichte anerkannter Dritter oder interne Prüfberichte heranziehen.

93. Die Due-Diligence-Prüfung von Dienstleistern erfolgt vor einer Auslagerung von IKT-Diensten und/oder IKT-Systemen. Wenn Finanzintermediäre eine zweite Vereinbarung mit einem Dienstleister schliessen, der bereits einer Prüfung unterzogen wurde, stellen Finanzintermediär auf der Grundlage eines risikobasierten Ansatzes fest, ob eine zweite Due-Diligence-Prüfung erforderlich ist.

94. Falls Finanzintermediäre Kenntnis von erheblichen Mängeln und/oder erheblichen Veränderungen in Bezug auf die erbrachten Dienstleistungen oder die Situation von Dienstleistern erlangen, ist die Due-Diligence-Prüfung umgehend zu überprüfen oder erneut durchzuführen.

10.6 Interessenkonflikt

95. Finanzintermediäre haben Interessenkonflikte hinsichtlich ihrer Auslagerungsvereinbarungen zu erkennen, zu bewerten und zu regeln. Wenn eine Auslagerung zu wesentlichen Interessenkonflikten führt, auch zwischen Einheiten innerhalb derselben Gruppe, müssen die Finanzintermediäre geeignete Massnahmen ergreifen, um diese Interessenkonflikte zu regeln.

10.7 Register der Auslagerungsvereinbarungen

96. Finanzintermediäre führen im Rahmen ihres Governance- und Risikomanagementsystems ein laufend aktualisiertes Register über Auslagerungsvereinbarungen. Unter Berücksichtigung der gesetzlichen Aufbewahrungsfristen führen Finanzintermediäre die Dokumentation von beendeten Auslagerungsvereinbarungen und die Begleitdokumentation für einen angemessenen Zeitraum weiterhin im Register.

10.8 Auslagerungsvereinbarung

97. Die Rechte und Pflichten des Finanzintermediärs und die Rechte und Pflichten des Dienstleisters sind eindeutig zuzuteilen und in einer schriftlichen Vereinbarung festzuhalten. Schnittstellen, Verantwortlichkeiten, Haftungsfragen sowie die Zuständigkeiten von Finanzintermediär und Dienstleister sind genau festzulegen und abzugrenzen und vertraglich zu regeln. Insbesondere ist zu formulieren, welche technischen und organisatorischen Sicherheitsmassnahmen ausgelagert werden und wie Finanzintermediäre die Wirksamkeit der ausgelagerten Kontrollen überwachen.

10.9 Weiterverlagerungen

98. In der Auslagerungsvereinbarung ist anzugeben, ob die Weiterverlagerung wichtiger IKT-Dienste und/oder IKT-Systeme zulässig ist oder nicht. Falls Weiterauslagerungen zulässig sind, sind die diesbezüglichen Bedingungen ebenfalls in der Auslagerungsvereinbarung festzuhalten. Zudem ist vertraglich sicherzustellen, dass die Auslagerungsvereinbarungen des Dienstleisters mit Subunternehmen im Einklang mit den vertraglichen Vereinbarungen der originären Auslagerungsvereinbarung stehen.

99. Der Dienstleister bleibt im Falle einer Weiterverlagerung auf ein Subunternehmen weiterhin gegenüber dem auslagernden Finanzintermediär berichtspflichtig. Der Dienstleister ist bei Auslagerung wichtiger IKT-Dienste und/oder IKT-Systeme zu verpflichten, die von ihm weiterverlagerten IKT-Dienste und/oder IKT-Systeme zu überwachen, um sicherzustellen, dass alle vertraglichen Pflichten zwischen dem Dienstleister und dem Finanzintermediär fortlaufend erfüllt werden.

100. Der Subunternehmer hat sich bei Auslagerung wichtiger IKT-Dienste und/oder IKT-Systeme vertraglich zu verpflichten alle geltenden Gesetze und vertraglichen Pflichten zu erfüllen und dem Finanzintermediär dieselben vertraglichen Zugangs-, Informations- und Prüfungsrechte einzuräumen, die vom Dienstleister gewährt werden.

10.10 Datensicherheit

101. Finanzintermediäre stellen sicher, dass Dienstleister geeignete IKT-Sicherheitsstandards einhalten.

102. Finanzintermediäre legen ein angemessenes Schutzniveau für die Vertraulichkeit von Daten, die Verfügbarkeit ausgelagerter IKT-Dienste und/oder IKT-Systeme und Daten sowie die Integrität und Rückverfolgbarkeit von Daten und Systemen im Rahmen der geplanten Auslagerung fest, welches im Einklang mit ihrer Informationssicherheitsleitlinie ist (Punkt 6.1 Informationssicherheitsleitlinie). Sofern dies für Daten bei der Übertragung, Daten im Speicher oder ruhende Daten erforderlich ist, ziehen Finanzintermediäre zudem spezielle Massnahmen in Betracht, wie den Einsatz von Verschlüsselungstechnologien in Kombination mit einer geeigneten Schlüsselmanagementarchitektur.

103. Um Vertraulichkeit, Verfügbarkeit und Integrität von ausgelagerten IKT-Diensten und IKT-Systemen zu gewährleisten, stellen Finanzintermediäre sicher, dass die Auslagerungsvereinbarungen (sowohl für den Normalfall als auch im Falle von Unterbrechungen (siehe auch 11.2 (Business Continuity Planning)) mit Dienstleistern bei Auslagerung wichtiger IKT-Dienste und/oder IKT-Systeme Folgendes umfassen:

a. angemessene und verhältnismässige Ziele und Massnahmen im Zusammenhang mit der Informationssicherheit einschliesslich Anforderungen wie:
    i. Mindestanforderungen an die Cybersicherheit, unter sinngemässer Berücksichtigung der Massnahmen nach Punkt 8.1 (Sicherheit des IKT-Betriebs),
    ii. Anforderungen an die Spezifikationen des Datenlebenszyklus des Finanzintermediärs
    iii. Anforderungen an die Datenverschlüsselung (at-rest und in-transit),
    iv. Anforderungen an Verfahren zur Überwachung der Netzwerksicherheit und Sicherheitsüberwachungsprozesse sowie den Standort von Rechenzentren. Finanzintermediäre stellen sicher, dass Dienstleister die ausgelagerten IKT-Dienste und IKT-Systeme sinngemäss nach Punkt 6.2 (Überwachung der IKT- und Informationssicherheit) überwachen,
    v. Anforderungen an Verfahren für logische Zugriffskontrollen / Zugriffschutz und physische Sicherheitsmassnahmen. Finanzintermediäre stellen sicher, dass Dienstleister sinngemäss nach Punkt 7. (Benutzerberechtigungsmanagement) die ausgelagerten IKT-Dienste und IKT-Systeme mittels logischen und physischen Sicherheitsverfahren schützen,
    vi. Anforderungen an Verfahren zur Überprüfung der Informationssicherheit. Finanzintermediäre stellen sicher, dass Dienstleister die Informationssicherheit in Bezug auf die ausgelagerten IKT-Dienste und IKT-Systeme sinngemäss nach Punkt 6.3 (Überprüfung, Bewertung und Testing der Informationssicherheit) überprüfen,
    vii. Anforderungen an Schulungsprogramme. Finanzintermediäre stellen sicher, dass Dienstleister ihre Mitarbeiter sinngemäss nach Punkt 6.4 (Schulung und Sensibilisierung für Informationssicherheit) schulen.
b. Prozesse zur Behandlung von Betriebs- und Sicherheitsvorfällen sinngemäss nach Punkt 8.2 (Management von IKT-Vorfällen und -Problemen), einschliesslich Eskalation und Berichterstattung gegenüber dem Finanzintermediär. Diese Prozesse haben Finanzintermediäre und Dienstleister periodisch gemeinsam zu testen.
c. Sicherung- und Wiederherstellungsverfahren sowie Verfahren zur Prüfung deren Wirksamkeit durch den Finanzintermediär sinngemäss nach Punkt 8 (IKT-Betriebsmanagement).

104. Finanzintermediäre überwachen die Einhaltung dieser Vorschriften und vergewissern sich über den Grad der Einhaltung der Sicherheitsziele, Massnahmen und Leistungsziele der Dienstleister durch vertraglich definierte Kennzahlen (Key Performance Indicators). Finanzintermediäre stellen vertraglich sicher, dass Dienstleister sie über Entwicklungen informieren müssen, die die ordnungsgemässe Erledigung der ausgelagerten Aktivitäten und Prozesse beeinträchtigen können.

10.11 Datenschutz

105. Bei Auslagerungen die den Umgang mit oder die Übertragung von personenbezogenen oder vertraulichen Daten umfassen, wählen Finanzintermediäre einen risikobasierten Ansatz betreffend den Standort bzw. die Standorte der Datenspeicherung und Datenverarbeitung (d. h. Land oder Region).

106. Finanzintermediäre stellen sicher, dass sie alle Anforderungen gemäss den für sie geltenden Datenschutzgesetzen auch in Bezug auf Auslagerungen von IKT-Diensten und/oder IKT-Systemen erfüllen. Bei Auslagerungen ins Ausland ist durch angemessene technische und organisatorische Massnahmen sicherzustellen, dass der Datenschutz nach den für sie geltenden Datenschutzgesetzen eingehalten wird.

107. Der Standort bzw. die Standorte der Datenspeicherung und Datenverarbeitung, einschliesslich des Standorts des oder der entsprechenden Rechenzentren, müssen dem Finanzintermediär bekannt sein.

10.12 Zugangs-, Informations- und Prüfungsrechte

108. Finanzintermediäre stellen im Rahmen der Auslagerungsvereinbarung jedenfalls für wichtige IKT-Dienste und/oder IKT-Systeme sicher, dass Dienstleister dem Finanzintermediär, seiner internen und externen Revisionsstelle und der FMA die Zugangs-, Informations- und Prüfungsrechte gewähren, die zur Überwachung der Auslagerungsvereinbarung und zur Einhaltung aller geltenden aufsichtsrechtlichen Anforderungen erforderlich sind. Dies ist vorbehaltlich weitergehender gesetzlicher Vorgaben zu sehen, welche für Finanzintermediäre gelten können. Finanzintermediäre stellen dies auch sicher, wenn die wichtigen IKT-Dienste und/oder IKT-Systeme an einen Dienstleister mit Sitz im Ausland ausgelagert werden oder wenn sie infolge der Auslagerung im Ausland erbracht werden.

109. Finanzintermediäre stellen bei der Auslagerung von wichtigen IKT-Diensten und/oder Systemen sicher, dass die Auslagerungsvereinbarung oder etwaige anderen vertraglichen Regelungen der wirksamen Ausübung der Zugangs-, Informations- und Prüfungsrechte durch die Finanzintermediäre, ihre interne oder externe Revisionsstelle oder die FMA nicht im Wege stehen oder diese einschränken.

110. Finanzintermediäre stellen Zugangs-, Informations- und Prüfungsrechte durch sie selbst, ihre interne oder externe Revisionsstelle oder die FMA im Falle einer Weiterverlagerung von wichtigen IKT-Diensten und/oder IKT-Systemen auch gegenüber Subunternehmen sicher.

111. Finanzintermediäre können bei der Auslagerung von wichtigen IKT-Diensten und/oder Systemen Erleichterungen wie das Heranziehen von Zertifizierungen Dritter, interne oder externe Prüfberichte sowie Sammelprüfungen in Anspruch nehmen, falls die für sie geltenden aufsichtsrechtlichen Anforderungen dies ermöglichen.

112. Finanzintermediäre stellen in der Auslagerungsvereinbarung sicher, dass die interne Revision in der Lage ist, die ausgelagerten IKT-Dienste und/oder IKT-Systeme im Rahmen eines risikobasierten Ansatzes zu prüfen.

10.13 Überwachung

113. Finanzintermediäre überwachen die Ausführung der Tätigkeiten, die Sicherheitsmassnahmen und die Einhaltung der vereinbarten Dienstleistungsgüte durch ihren Dienstleister regelmässig auf der Grundlage eines risikobasierten Ansatzes. Finanzintermediäre verwenden Verfahren, um die Einhaltung der an Dienstleister ausgelagerten Sicherheitskontrollen zu überwachen.

114. Das Leitungsorgan ist in regelmässigen Abständen auf den aktuellen Stand hinsichtlich der Risiken zu bringen, die in Bezug auf die Auslagerung von wichtigen IKT-Diensten und/oder IKT-Systemen ermittelt wurden. Die internen Verfahren der Finanzintermediäre stellen eine angemessene interne Berichterstattung im Zusammenhang mit der Auslagerung und Weiterverlagerungen von IKT-Diensten und/oder IKT-Systemen sicher.

115. Zum Zweck der Überwachung führt der Finanzintermediär Überwachungs- und Kontrollmechanismen ein, bei denen berücksichtigt wird, dass wichtige IKT-Dienste und/oder IKT-Systeme oder Teile davon weiterausgelagert wurden. Die Überwachungs- und Kontrollmechanismen beinhalten Indikatoren bezüglich der Ereignisse, die die Aktivierung der Ausstiegsstrategie auslösen könnten. Falls Mängel ermittelt werden, ergreifen die Finanzintermediäre geeignete Korrektur- oder Abhilfemassnahmen.

116. Finanzintermediäre vereinbaren in der Auslagerungsvereinbarung Weisungsrechte, welche sicherstellen, dass alle erforderlichen und zur Erfüllung der vereinbarten Dienstleistung notwendigen Weisungen erteilt werden können, um eine Einflussnahme- und Steuerungsmöglichkeit für den Finanzintermediär auf die ausgelagerten IKT-Diensten und/oder IKT-Systemen zu schaffen.

10.14 Business Continuity für ausgelagerte ITK Dienste und/oder Systeme

117. Finanzintermediäre erstellen sinngemäss nach Punkt 11 (Notfallkonzept und Business Continuity Management) geeignete Business Continuity Pläne hinsichtlich ausgelagerter wichtiger IKT-Dienste und/oder IKT-Systeme, pflegen diese und testen sie regelmässig. Dabei berücksichtigen sie Szenarien wie die Verschlechterung der Qualität der Erbringung der ausgelagerten wichtigen IKT-Dienste und/oder IKT-Systeme auf ein inakzeptables Niveau, die Unterlassung ihre Erbringung, möglichen Auswirkungen der Insolvenz oder eines anderen Ausfalls von Dienstleistern sowie gegebenenfalls politische Risiken in der Rechtsordnung des Dienstleisters.

10.15 Ausstiegsstrategien

118. Bei der Auslagerung von wichtigen IKT-Diensten und/oder IKT-Systemen verfügen Finanzintermediäre über eine dokumentierte Ausstiegsstrategie, die mit ihrer Auslagerungsrichtlinie und den Business Continuity Plänen in Einklang steht und auf ihre Durchführbarkeit geprüft wird.

119. Es sind für die Ausstiegsstrategie mindestens folgende Möglichkeiten zu berücksichtigen:

a. die Kündigung der Auslagerungsvereinbarung (ordentlich oder fristlos);
b. der Ausfall des Dienstleisters;
c. die Verschlechterung der Qualität der ausgeführten Dienstleistung und tatsächliche oder potenzielle betriebliche Störungen aufgrund der unangemessenen oder unterlassenen Ausführung der Dienstleistung;
d. das Entstehen wesentlicher Risiken für die angemessene und fortlaufende Anwendung der Dienstleistung.

120. Finanzintermediäre vereinbaren in der Auslagerungsvereinbarung eine eindeutig formulierte Klausel, die ihnen die Kündigung der Auslagerungsvereinbarung ermöglicht sowie angemessene Kündigungsfristen. Die Kündigung der Auslagerung von wichtigen IKT-Diensten und/oder IKT-Systemen sollte unbeschadet der Kontinuität und der Qualität der Dienstleistungserbringung der Finanzintermediäre gegenüber ihren Kunden möglich sein.

121. Finanzintermediäre stellen eine Rückführung der ausgelagerten wichtigen IKT-Dienste und/oder IKT-Systeme unter Berücksichtigung der System- und Datenformatkompatibilität sicher. Finanzintermediäre stellen ebenfalls sicher, dass Dienstleister sie bei der Übertragung der ausgelagerten wichtigen IKT-Dienste und/oder IKT-Systeme, Daten oder Anwendungen an einen anderen Dienstleister oder direkt an die Finanzintermediäre angemessen unterstützt und dass der Dienstleister die Daten des Finanzintermediärs nach der (Rück-) Übertragung vollständig und sicher löschen wird.

11. Notfallkonzept und Business Continuity Management

122. Finanzintermediäre richten ein Business Continuity Management (BCM) ein, um ihre Fähigkeit zur kontinuierlichen Erbringung von Dienstleistungen zu maximieren und Verluste im Falle von schwerwiegenden Betriebsstörungen zu begrenzen.

123. Die Verfahren zum Business Continuity Management werden im Prüfplan der internen Revision angemessen berücksichtigt.

11.1 Business-Impact-Analyse (BIA)

124. Im Rahmen des Business Continuity Managements führen Finanzintermediäre Business Impact Analysen (BIA) durch, indem sie ihre Exposition gegenüber schwerwiegenden Geschäftsstörungen und Bewertung der potenziellen Auswirkungen (einschliesslich auf Vertraulichkeit, Integrität und Verfügbarkeit), quantitativ und qualitativ analysieren, unter Verwendung interner und/oder externer Daten (z.B. Daten von Dienstleistern, welche für einen Geschäftsprozess relevant sind oder öffentlich zugängliche Daten, die für die BIA relevant sein können) und Szenarioanalysen. Der Finanzintermediär stellt sicher, dass bei den Szenarioanalysen alle Geschäftsbereiche und interne Einheiten bzw. Prozesse sowie Auslagerungen miteinbezogen werden. Die BIA berücksichtigt auch die Kritikalität der identifizierten und klassifizierten Geschäftsfunktionen, Unterstützungsprozesse, Drittparteien und IKT-Assets sowie deren gegenseitige Abhängigkeiten gemäss 5.3 (Einstufung der Kritikalität und Risikobewertung).

125. Der Finanzintermediär sorgt für eine angemessene und regelmässige Durchführung der BIA. Der Finanzintermediär legt zudem Kriterien fest, nach denen ad-hoc Business Impact Analysen ausserhalb des normalen Aktualisierungszyklus durchzuführen sind.

126. Finanzintermediäre stellen sicher, dass ihre IKT-Systeme und IKT-Dienste so konzipiert und auf die BIA abgestimmt sind, dass z.B. bestimmte kritische Komponenten (siehe auch 5.3 Einstufung der Kritikalität und Risikobewertung) redundant ausgelegt sind, um Störungen durch Ereignisse mit Auswirkungen auf diese Komponenten zu verhindern.

11.2 Business Continuity Planning

127. Auf der Grundlage ihrer BIA stellen Finanzintermediäre Pläne zur Gewährleistung der Geschäftskontinuität auf (Business Continuity Pläne, BCPs), die vom Leitungsorgan dokumentiert und genehmigt werden. Die Pläne berücksichtigen insbesondere Risiken, die sich nachteilig auf die Weiterführung der Geschäftsaktivitäten auswirken könnten. Die Pläne unterstützen den Schutz und erforderlichenfalls die Wiederherstellung der Vertraulichkeit, Integrität und Verfügbarkeit ihrer Geschäftsfunktionen, Unterstützungsprozesse und IKT-Assets. Finanzintermediäre stimmen sich gegebenenfalls mit relevanten internen und externen Akteuren bei der Aufstellung dieser Pläne ab.

128. Finanzintermediäre richten BCPs ein, um sicherzustellen, dass sie angemessen auf potenzielle Ausfallszenarien reagieren können und dass sie in der Lage sind, den Betrieb ihrer kritischen Geschäftsaktivitäten nach Störungen innerhalb einer vorgegebenen Wiederherstellungszeit (Recovery Time Objectives - RTO, die maximale Zeit innerhalb derer ein System oder Prozess nach einem Vorfall wiederhergestellt werden muss) und zu einem vorgegebenen Wiederherstellungspunkt (Recovery Point Objetive - RPO, der maximale Zeitraum, in dem ein Datenverlust im Falle eines Vorfalls akzeptabel ist) wiederherzustellen. RTO und RPO sind auch mit Dienstleistern in Bezug auf ausgelagerte wichtige IKT-Dienste und/oder Systeme zu vereinbaren. In Fällen schwerwiegender Betriebsstörungen, die bestimmte BCPs auslösen, priorisieren Finanzintermediäre Massnahmen zur Aufrechterhaltung des Geschäftsbetriebs mit einem risikobasierten Ansatz, welcher sich auf die Risikobewertung in 5.3 (Einstufung der Kritikalität und Risikobewertung) stützt.

129. Ein Finanzintermediär berücksichtigt in seinem BCP eine Reihe verschiedener Szenarien, einschliesslich extreme, aber plausible Szenarien, denen sie ausgesetzt sein könnten, sowie Cyber-Angriffsszenarien. Zudem bewerten sie die möglichen Auswirkungen solcher Szenarien. Basierend auf diesen Szenarien, beschreibt ein Finanzintermediär, wie die Kontinuität von IKT-Systemen und -Diensten sowie die Informationssicherheit des Finanzintermediärs gewährleistet werden.

130. Der Finanzintermediär schult Mitarbeitende betreffend die Notfallpläne.

11.3 Reaktions- und Wiederherstellungspläne

131. Basierend auf den BIAs und plausiblen Szenarien, entwickeln Finanzintermediäre Reaktions- und Wiederherstellungspläne. In diesen Plänen wird festgelegt, unter welchen Bedingungen die Pläne aktiviert werden können und welche Massnahmen ergriffen werden, um die Verfügbarkeit, Kontinuität und Wiederherstellung zumindest der kritischen IKT-Systeme und IKT-Dienste des Finanzintermediärs zu gewährleisten. Mit den Reaktions- und Wiederherstellungsplänen werden die Wiederherstellungsziele des Finanzintermediärs erreicht.

132. Die Reaktions- und Wiederherstellungspläne berücksichtigen sowohl kurzfristige als auch langfristige Wiederherstellungsmöglichkeiten. Die Pläne:

a) konzentrieren sich auf die Wiederherstellung des Betriebs kritischer Geschäftsfunktionen, Unterstützungsprozesse, IKT-Assets und deren gegenseitigen Abhängigkeiten, um nachteilige Auswirkungen auf die Funktionsweise der Finanzintermediäre und des Finanzsystems zu vermeiden
b) werden dokumentiert und den Geschäfts- und Unterstützungseinheiten zur Verfügung gestellt und sind im Falle eines Notfalls leicht zugänglich;
c) werden entsprechend den Erkenntnissen aus Vorfällen, Tests, neu identifizierten Risiken und Bedrohungen, und veränderten Wiederherstellungszielen und -prioritäten aktualisiert.

133. Die Pläne ziehen auch alternative Optionen in Betracht, bei denen eine Wiederherstellung kurzfristig aufgrund von Kosten, Risiken, Logistik oder unvorhergesehenen Umständen möglicherweise nicht möglich ist.

134. Darüber hinaus berücksichtigt und führt ein Finanzintermediär im Rahmen der Reaktions- und Wiederherstellungspläne Kontinuitätsmassnahmen ein, um Ausfälle von Dienstleistern zu mindern, welche von zentraler Bedeutung für die Kontinuität der IKT-Dienste eines Finanzintermediärs sind.

11.4 Testen von Plänen

135. Finanzintermediäre testen ihre BCPs regelmässig. Insbesondere stellen sie sicher, dass die BCPs ihrer kritischen Geschäftsfunktionen, Unterstützungsprozesse, IKT-Assets und ihrer Interdependenzen (einschliesslich der von Dritten bereitgestellten, sofern zutreffend) regelmässig und gegebenenfalls graduell getestet werden.

136. Die BCPs werden mindestens einmal jährlich auf der Grundlage der Testergebnisse, der aktuellen Bedrohungsinformationen und Lehren aus früheren Ereignissen aktualisiert. Die betroffenen Bereiche und Mitarbeitenden werden über die Aktualisierung informiert. Jegliche Änderungen der Wiederherstellungsziele (einschliesslich RTOs und RPOs) und/oder Änderungen der Geschäftsfunktionen, Unterstützungsprozesse und IKT-Assets, werden sofern relevant auch als Grundlage für die Aktualisierung der BCPs herangezogen.

137. Die Prüfung der BCPs durch Finanzintermediäre weist nach, dass sie in der Lage sind, die Funktionsfähigkeit ihrer Geschäfte zu erhalten, bis die kritischen Tätigkeiten wiederhergestellt sind. Insbesondere:

a) umfassen sie Prüfungen einer angemessenen Reihe schwerwiegender, aber plausibler Szenarien, einschliesslich solcher welche für die Entwicklung der BCPs berücksichtigt wurden (sowie das Testen von Systemen zur Verfügung gestellt durch Dritte, sofern anwendbar); Dies beinhaltet die Umstellung der kritischen Geschäftsfunktionen, Unterstützungsprozesse und IKT-Assets zur Notfallwiederherstellungsumgebung und zeigen, dass sie auf diese Weise für eine ausreichend repräsentative Zeitspanne ausgeführt werden können und dass die normale Funktion danach wiederhergestellt werden kann;
b) sind sie darauf ausgelegt, die Annahmen in Frage zu stellen, auf denen die BCPs beruhen, einschliesslich der Governance-Regelungen und Krisenkommunikationspläne;
c) beinhalten sie Verfahren zur Überprüfung der Fähigkeiten ihrer Mitarbeiter, Auftragnehmer, Dienstleister, IKT-Systeme und IKT-Dienste, angemessen auf die definierten Szenarien zu reagieren.

138. Die Testergebnisse werden dokumentiert und alle festgestellten Mängel, die sich aus den Tests ergeben, werden analysiert, adressiert und dem Leitungsorgan gemeldet.

11.5 Krisenkommunikation

139. Im Falle einer Störung oder eines Notfalls und während der Umsetzung der BCPs sorgen Finanzintermediäre dafür, dass sie über angemessene und wirksame Massnahmen zur Krisenkommunikation verfügen, damit alle relevanten internen und externen Akteure, einschliesslich der zuständigen Behörden, wenn vorgeschrieben durch nationale Vorschriften, sowie relevante Dienstleister rechtzeitig und angemessen informiert werden.

140. Die FMA erwartet ferner, dass die Finanzintermediäre die FMA innert 7 Tagen ab Kenntniserlangung über schwerwiegende oder betriebsstörende Cyber-Attacken informieren.

12. Datenschutz

Die FMA verarbeitet personenbezogene Daten ausschliesslich nach den allgemeinen Datenverarbeitungsgrundsätzen der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG) sowie nach dem geltenden Datenschutzrecht.

Sämtliche Informationen zur Verarbeitung personenbezogener Daten, einschliesslich der Angaben zum Verarbeitungszweck, zum Datenverantwortlichen sowie zu den Betroffenenrechten sind in der FMA-Information zum Datenschutz enthalten: https://www.fma-li.li/de/fma/datenschutz/fma-information-zum-datenschutz.html

13. Inkraftsetzung

Diese Richtlinie wurde vom Aufsichtsrat der FMA am 19. Mai 2021 genehmigt und tritt am 1. Januar 2022 in Kraft.

Für Rückfragen steht die FMA zur Verfügung.
Telefon: +423 236 73 73
E-Mail: info@fma-li.li