Leitlinien

EBA/GL/2019/04

28. November 2019

EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken

Einhaltung der Vorschriften und Meldepflichten

Status dieser Leitlinien

1. Das vorliegende Dokument enthält Leitlinien, die gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010 herausgegeben wurden.[1] Gemäß Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden und Finanzinstitute alle erforderlichen Anstrengungen unternehmen, um diesen Leitlinien nachzukommen.

2. Die Leitlinien legen fest, was nach Ansicht der EBA angemessene Aufsichtspraktiken innerhalb des Europäischen Finanzaufsichtssystems sind oder wie das Unionsrecht in einem bestimmten Bereich anzuwenden ist. Die zuständigen Behörden im Sinne von Artikel 4 Absatz 2 der Verordnung (EU) Nr. 1093/2010, für die die Leitlinien gelten, sollten diese Leitlinien einhalten, indem sie sie gegebenenfalls in der Praxis einsetzen (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsprozesse), auch wenn sich die Leitlinien in erster Linie an Institute richten.

Meldepflichten

3. Nach Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden der EBA bis zum ([TT.MM.JJJJ]) mitteilen, ob sie diesen Leitlinien nachkommen oder nachzukommen beabsichtigen, oder die Gründe nennen, warum sie dies nicht tun. Geht innerhalb der genannten Frist keine Mitteilung ein, geht die EBA davon aus, dass die zuständige Behörde den Anforderungen nicht nachkommt. Die Mitteilungen sind unter Verwendung des auf der Website der EBA abrufbaren Formulars mit dem Betreff „EBA/GL/2019/04“ an compliance@eba.europa.eu zu senden. Die Meldungen sollten durch Personen erfolgen, die befugt sind, entsprechende Meldungen im Auftrag ihrer Behörde zu übermitteln. Jegliche Änderungen des Status der Einhaltung müssen der EBA ebenfalls gemeldet werden.

4. Die Meldungen werden gemäß Artikel 16 Absatz 3 der EBA-Verordnung auf der Website der EBA veröffentlicht.

[1] Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12).

Gegenstand, Anwendungsbereich und Begriffsbestimmungen

Gegenstand

5. Diese Leitlinien stützen sich auf die Bestimmungen von Artikel 74 der Richtlinie 2013/36/EU (CRD) in Bezug auf die interne Governance und ergeben sich aus dem Mandat zur Veröffentlichung von Leitlinien gemäß Artikel 95 Absatz 3 der Richtlinie (EU) 2015/2366 (PSD2).

6. Diese Leitlinien legen die Maßnahmen für das Management von Risiken fest, die Finanzinstitute (wie in Absatz 9 unten festgelegt) gemäß Artikel 74 der CRD für die Verwaltung ihrer IKT- und Sicherheitsrisiken für alle Tätigkeiten ergreifen müssen und die Zahlungsdienstleister (ZDL, wie in Absatz 9 festgelegt) gemäß Artikel 95 Absatz 1 der PSD2, übernehmen müssen, um die operationellen und sicherheitsrelevanten Risiken („IKT- und Sicherheitsrisiken“) in Bezug auf die von ihnen erbrachten Zahlungsdienste zu beherrschen. Die Leitlinien umfassen Anforderungen an die Informationssicherheit, einschließlich Cybersicherheit, soweit die Informationen auf IKT-Systemen gehalten werden.

Anwendungsbereich

7. Diese Leitlinien gelten für das Management von IKT- und Sicherheitsrisiken innerhalb von Finanzinstituten (wie in Absatz 9 festgelegt). Zum Zwecke dieser Leitlinien bezieht sich der Begriff „IKT- und Sicherheitsrisiken“ auf die operationellen und sicherheitsrelevanten Risiken im Sinne von Artikel 95 der PSD2 für die Erbringung von Zahlungsdiensten.

8. Für Zahlungsdienstleister (im Sinne von Absatz 9) gelten diese Leitlinien für ihre Erbringung von Zahlungsdiensten im Einklang mit dem Umfang und Mandat von Artikel 95 der PSD2. Für Institute (wie in Absatz 9 festgelegt) gelten diese Leitlinien für alle von ihnen angebotenen Tätigkeiten.

Adressaten

9. Diese Leitlinien richten sich an Finanzinstitute, nämlich für die Zwecke dieser Leitlinien an (1) Zahlungsdienstleister im Sinne von Artikel 4 Absatz 11 der PSD2 und (2) Institute, d. h. Kreditinstitute und Wertpapierfirmen im Sinne von Artikel 4 Absatz 1 Ziffer 3 der Verordnung (EU) Nr. 575/2013. Die Leitlinien gelten auch für die zuständigen Behörden im Sinne von Artikel 4 Absatz 1 Ziffer 40 der Verordnung (EU) Nr. 575/2013, einschließlich der Europäischen Zentralbank in Zusammenhang mit der Wahrnehmung der ihr durch die Verordnung (EU) Nr. 1024/2013 übertragenen Aufgaben, sowie an zuständige Behörden gemäß der PSD2 im Sinne von Artikel 4 Absatz 2 Ziffer i der Verordnung (EU) Nr. 1093/2010.

Begriffsbestimmungen

10. Sofern nicht anders angegeben, haben die in der Richtlinie 2013/36/EU (CRD), der Verordnung (EU) Nr. 575/2013 (CRR) und der Richtlinie (EU) 2015/2366 (PSD2) verwendeten und definierten Begriffe in diesen Leitlinien dieselbe Bedeutung. Für die Zwecke dieser Leitlinien gelten darüber hinaus die folgenden Begriffsbestimmungen:

IKT- und Sicherheitsrisiko	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) [2] . Dies umfasst Sicherheitsrisiken, die aus unzulänglichen oder fehlgeschlagenen internen Prozessen oder externen Ereignissen resultieren, einschließlich Cyber-Attacken oder unzureichender physischer Sicherheit.
Leitungsorgan	a) Für Kreditinstitute und Wertpapierfirmen hat dieser Begriff die gleiche Bedeutung wie die Definition gemäß Artikel 3 Absatz 1 Ziffer 7 der Richtlinie 2013/36/EU. b) Für Zahlungsinstitute oder E-Geld-Institute umfasst dieser Begriff Geschäftsleiter oder Personen, die für die Geschäftsleitung der Zahlungs- und E-Geld-Institute verantwortlich sind, sowie gegebenenfalls Personen, die für das Management der Zahlungsdienstgeschäfte der Zahlungs- und E-Geld-Institute verantwortlich sind. c) Für Zahlungs- und E-Geld-Institute gemäß Artikel 1 Absatz 1 Buchstaben c, e und f der Richtlinie (EU) 2015/2366 hat dieser Begriff die ihm gemäß den geltenden EU- oder nationalen Rechtsvorschriften zugewiesene Bedeutung.
Betriebs- oder Sicherheitsvorfall	Ein einzelnes Ereignis oder eine Reihe zusammenhängender Ereignisse, die vom Finanzinstitut nicht geplant wurden und sich negativ auf die Integrität, Verfügbarkeit, Vertraulichkeit und/oder Authentizität von Diensten auswirken oder auswirken könnten.
Geschäftsleitung	a) Für Kredit- und E-Geld-Institute hat dieser Begriff die gleiche Bedeutung wie die Definition gemäß Artikel 3 Absatz 1 Nummer 9 der Richtlinie 2013/36/EU. b) Für Zahlungs- und E-Geld-Institute umfasst dieser Begriff natürliche Personen, die Führungspositionen in einem Institut übernehmen und die für die Leitung des Tagesgeschäfts des

[2] Definition aus den EBA-Leitlinien zu gemeinsamen Verfahren und Methoden für den aufsichtlichen Überprüfungs- und Bewertungsprozess vom 19. Dezember 2014 (EBA/GL/2014/13), geändert durch EBA/GL/2018/03.

	Instituts verantwortlich und gegenüber dem Leitungsorgan rechenschaftspflichtig sind. c) Für Zahlungsdienstleister gemäß Artikel 1 Absatz 1 Buchstaben c, e und f der Richtlinie (EU) 2015/2366 hat dieser Begriff die ihm gemäß den geltenden EU- oder nationalen Rechtsvorschriften zugewiesene Bedeutung.
Risikoappetit	Das Gesamtniveau und die Arten von Risiken, welche die Zahlungsdienstleister und Institute bereit sind, innerhalb ihrer Risikokapazität und im Einklang mit ihren Geschäftsmodell einzugehen, um ihre strategischen Ziele zu erreichen.
Interne Revision	a) Für Kreditinstitute und Wertpapierfirmen wird die Interne Revision in Abschnitt 22 der EBA-Leitlinien zur internen Governance (EBA/GL/2017/11) beschrieben. b) Für Zahlungsdienstleister, die keine Kreditinstitute sind, muss die Interne Revision innerhalb der Organisation des Zahlungsdienstleisters oder vom Zahlungsdienstleister unabhängig sein und kann eine interne und/oder externe Revision sein.
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.
Dritte	Jede Organisation, die Geschäftsbeziehungen oder Verträge mit einem Unternehmen eingegangen ist, um ein Produkt oder eine Dienstleistung zu liefern bzw. zu erbringen[3].
Datenbestand	Eine Sammlung an schützenswerten materiellen oder immateriellen Informationen.
IKT-Asset	Ein Bestand aus Software oder Hardware, die man im Unternehmensumfeld findet.
IKT-Systeme[4]	IKT-Komponenten als Teil eines Verbunds oder eines verbundenen Netzwerks, das die Betriebsaktivitäten eines Finanzinstituts unterstützt.
IKT-Dienste[5]	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.

[3] Definition der grundlegenden G7-Grundelemente zur effektiven Bewertung der Cybersicherheit im Finanzsektor.
[4] Definition aus den Leitlinien für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (SREP) (EBA/GL/2017/05).
[5] ibid.

Umsetzung

Beginn der Anwendung

11. Diese Leitlinien gelten ab dem 30. Juni 2020.

Aufhebung

12. Die 2017 herausgegebenen Leitlinien zu Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken (EBA/GL/2017/17) werden zum Zeitpunkt des Inkrafttretens dieser Leitlinien durch diese Leitlinien aufgehoben.

Leitlinien für das Management von IKT- und Sicherheitsrisiken

1.1. Proportionalität

1. Alle Finanzinstitute sollten die Bestimmungen dieser Leitlinien in einer Weise befolgen, die der Größe der Finanzinstitute, ihrer internen Organisation und der Art und dem Umfang der Finanzinstitute, der Komplexität und dem Risikogehalt der Dienstleistungen und Produkte, welche die Finanzinstitute erbringen oder bereitzustellen beabsichtigen, angemessen ist und diese berücksichtigt.

1.2. Governance und Strategie

1.2.1. Governance

2. Das Leitungsorgan sollte sicherstellen, dass die Finanzinstitute über eine angemessene interne Governance sowie einen internen Kontrollrahmen für ihre IKT- und Sicherheitsrisiken verfügen. Das Leitungsorgan sollte klare Aufgaben und Zuständigkeiten für IKT-Funktionen, das Informationssicherheitsrisikomanagement und die Geschäftsfortführung bestimmen, einschließlich derjenigen für das Leitungsorgan und seine Ausschüsse.

3. Das Leitungsorgan sollte sicherstellen, dass die Anzahl und Fähigkeiten des Personals von Finanzinstituten angemessen sind, damit ihre IKT-Betriebsbedürfnisse und ihre IKT- und Sicherheitsrisikomanagementprozesse und die Umsetzung ihrer IKT-Strategie laufend gewährleistet werden können. Das Leitungsorgan sollte außerdem sicherstellen, dass das zugewiesene Budget für die Erfüllung der oben genannten Aspekte angemessen ist. Zudem sollten die Finanzinstitute sicherstellen, dass das gesamte Personal, einschließlich Inhaber von Schlüsselfunktionen, jährlich oder bei Bedarf häufiger eine angemessene Schulung für Informationssicherheit, IKT- und Sicherheitsrisiken erhält (siehe Abschnitt 3.4.7).

4. Dem Leitungsorgan obliegt die Gesamtverantwortung für die Festlegung, Genehmigung und Überwachung der Umsetzung der IKT-Strategie der Finanzinstitute als Teil ihrer gesamten Unternehmensstrategie sowie für die Schaffung eines wirksamen Risikomanagementrahmens für die IKT- und Sicherheitsrisiken.

1.2.2. Strategie

5. Die IKT-Strategie sollte sich an der Geschäftsstrategie ausrichten und Folgendes festlegen:
   a) wie sich die IKT der Finanzinstitute entwickeln sollten, um ihre Geschäftsstrategie, einschließlich der Entwicklung der Organisationsstruktur, der Änderungen von IKT-Systemen und wichtiger Abhängigkeiten mit Dritten, wirksam zu unterstützen und dazu beizutragen;
   b) die geplante Strategie und Entwicklung der IKT-Architektur, einschließlich Abhängigkeiten von Dritten;
   c) klare Informationssicherheitsziele, die sich auf IKT-Systeme und IKT-Dienste, -Personal und -Prozesse konzentrieren.

6. Die Finanzinstitute sollten Maßnahmenpläne aufstellen, in denen die Ziele zur Erreichung der IKT-Strategie, festgelegt werden. Diese sollten dem gesamten betroffenen Personal (einschließlich Auftragnehmern und Dritten, falls zutreffend und relevant) mitgeteilt werden. Die Maßnahmenpläne sollten periodisch überprüft werden, um ihre Relevanz und Angemessenheit sicherzustellen. Die Finanzinstitute sollten zudem Prozesse einführen, um die Wirksamkeit der Umsetzung ihrer IKT-Strategie zu überwachen und zu messen.

1.2.3. Nutzung von Drittanbietern

7. Unbeschadet der EBA-Leitlinien zu Auslagerungen (EBA/GL/2019/02) und Artikel 19 der PSD2 sollten die Finanzinstitute die Wirksamkeit der in ihrem Risikomanagementrahmen festgelegten Maßnahmen zur Risikominderung, einschließlich der in diesen Leitlinien dargelegten Maßnahmen, gewährleisten, wenn operative Funktionen im Zusammenhang mit Zahlungsdiensten und/oder IKT-Diensten und IKT-Systemen jeglicher Tätigkeit ausgelagert werden, einschließlich an Gruppenunternehmen, oder wenn Dritte herangezogen werden.

8. Um die Verfügbarkeit von IKT-Diensten und IKT-Systemen zu gewährleisten, sollten die Finanzinstitute sicherstellen, dass Verträge und Dienstleistungsvereinbarungen (sowohl unter normalen Umständen als auch im Fall von Störungen der Dienste – siehe auch Abschnitt 3.7.2) mit den Anbietern (Outsourcing-Anbieter, Gruppenunternehmen oder Drittanbieter) Folgendes umfassen:
   a) angemessene und verhältnismäßige Ziele und Maßnahmen im Zusammenhang mit der Informationssicherheit, einschließlich Mindestanforderungen an die Cybersicherheit, Anforderungen an den Lebenszyklus der Daten des Finanzinstituts, sämtliche Anforderungen hinsichtlich der Datenverschlüsselung, der Verfahren zur Überwachung der Netzwerksicherheit und der Sicherheit, und des Standorts von Rechenzentren;
   b) Prozesse zur Handhabung von Betriebs- und Sicherheitsvorfällen, einschließlich Eskalation und Meldung.

9. Die Finanzinstitute sollten diese Dienstleister im Hinblick auf Sicherheitsziele, -maßnahmen und Erfüllung der vereinbarten Leistung überwachen.

1.3. Rahmenwerk für das Management von IKT- und Sicherheitsrisiken

1.3.1. Organisation und Ziele

10. Die Finanzinstitute sollten ihre IKT- und Sicherheitsrisiken identifizieren und steuern. Die -Funktion(en) bzw. Organisationseinheiten, die für IKT-Systeme, -Prozesse und -Sicherheitsmaßnahmen zuständig sind, sollten über geeignete Verfahren und Kontrollen verfügen, um sicherzustellen, dass alle Risiken ermittelt, analysiert, gemessen, überwacht, verwaltet, gemeldet und innerhalb der Grenzen der Risikobereitschaft des Finanzinstituts gehalten werden und dass die von ihnen durchgeführten Projekte und bereitgestellten Systeme sowie die durchgeführten Tätigkeiten den externen und internen Anforderungen entsprechen.

11. Die Finanzinstitute sollten die Zuständigkeit für das Management und die Überwachung von IKT- und Sicherheitsrisiken einer Kontrollfunktion übertragen, wobei die Anforderungen von Abschnitt 19 der EBA-Leitlinien zur internen Governance (EBA/GL/2017/11) einzuhalten sind. Die Finanzinstitute sollten die Unabhängigkeit und Objektivität dieser Kontrollfunktion dadurch gewährleisten, dass eine angemessene Trennung von den IKT-Betriebsprozessen sichergestellt ist. Diese Kontrollfunktion sollte gegenüber dem Leitungsorgan unmittelbar rechenschaftspflichtig und für die Überwachung und Kontrolle der Einhaltung des IKT- und Sicherheitsrisikomanagementrahmenwerks zuständig sein. Sie sollte sicherstellen, dass die IKT- und Sicherheitsrisiken identifiziert, gemessen, bewertet, verwaltet, überwacht und berichtet werden. Die Finanzinstitute sollten sicherstellen, dass diese Kontrollfunktion nicht für die interne Revision zuständig ist.

    Die interne Revision sollte 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, wobei die Anforderungen von Abschnitt 22 der EBA-Leitlinien zur internen Governance (EBA/GL/2017/11) einzuhalten sind.

12. Die Finanzinstitute sollten Schlüsselrollen und Verantwortlichkeiten, sowie entsprechende Berichtspflichten festlegen und zuweisen, damit das IKT- und Informationssicherheitsrisikomanagement wirksam ist. Dieser Rahmen sollte vollständig in die gesamten Risikomanagementprozesse der Finanzinstitute integriert und auf diese abgestimmt werden.

13. Das IKT- und Informationssicherheitsrisikomanagement sollte Prozesse beinhalten, um

    a) die Risikobereitschaft von IKT- und Sicherheitsrisiken in Übereinstimmung mit der Risikobereitschaft des Finanzinstituts zu bestimmen;
    b) IKT- und Sicherheitsrisiken, denen das Finanzinstitut ausgesetzt ist, festzustellen und zu bewerten;
    c) Maßnahmen, einschließlich Kontrollen, zur Minderung von IKT- und Sicherheitsrisiken festzulegen;
    d) die Wirksamkeit dieser Maßnahmen sowie die Zahl der gemeldeten Vorfälle, einschließlich der gemeldeten Vorfälle für Zahlungsdienstleister laut Artikel 96 der PSD2, die sich auf die IKT-bezogenen Aktivitäten auswirken, zu überwachen und bei Bedarf Maßnahmen zu ergreifen;
    e) dem Leitungsorgan über IKT- und Sicherheitsrisiken und Kontrollen zu berichten;
    f) festzustellen und zu beurteilen, ob es IKT- und Sicherheitsrisiken gibt, die auf eine größere Änderung des IKT-Systems oder der IKT-Dienste, -Prozesse oder -Verfahren und/oder einen erheblichen Betriebs- oder Sicherheitsvorfall zurückzuführen sind.

14. Die Finanzinstitute sollten sicherstellen, dass das IKT- und Informationssicherheitsrisikomanagement auf Grundlage der gewonnenen Erfahrungen während der Umsetzung und Überwachung dokumentiert und laufend verbessert wird. Das IKT- und Informationssicherheitsrisikomanagement sollte vom Leitungsorgan genehmigt und mindestens jährlich überprüft werden.

1.3.2. Ermittlung von Funktionen, Prozessen und IT-Assets

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

16. Darüber hinaus sollten die Finanzinstitute eine aktualisierte Übersicht über die IT-Assets, die ihre geschäftliche Funktionen, Aufgaben, Geschäfts- und Unterstützungsprozesse unterstützen, wie z. B. IKT-Systeme, Mitarbeiter, Auftragnehmer, Dritte und Abhängigkeiten von anderen internen und externen Systemen und Prozessen, ermitteln, einrichten und auf dem neuesten Stand halten, um zumindest die IT-Assets verwalten zu können, die ihre kritischen Geschäftsfunktionen und -prozesse unterstützen.

1.3.3. Klassifizierung und Risikobewertung

17. Die Finanzinstitute sollten die in den Absätzen 15 und 16 genannten ermittelten Geschäftsfunktionen, Unterstützungsprozesse und IT-Assets im Hinblick auf ihre Kritikalität einstufen.

18. Bei der Festlegung der Kritikalität dieser festgestellten Geschäftsfunktionen, Unterstützungsprozesse und IT-Assets sollten die Finanzinstitute mindestens die Anforderungen bezüglich Vertraulichkeit, Integrität und Verfügbarkeit berücksichtigen. Es sollten klar zugewiesene Zuständigkeiten und Verantwortlichkeiten für die IT-Assets vorliegen.

19. Die Finanzinstitute sollten bei der Risikobewertung die Angemessenheit der Klassifizierung der IT-Assets und die entsprechende Dokumentation überprüfen.

20. Die Finanzinstitute sollten die IKT- und Sicherheitsrisiken entsprechend ihrer Kritikalität ermitteln, die sich auf die festgestellten und klassifizierten Geschäftsfunktionen, Unterstützungsprozesse und IT-Assets auswirken. Die Risikobewertung sollte jährlich oder, falls erforderlich, in kürzeren Zeitabständen durchgeführt und dokumentiert werden. Derartige Risikobewertungen sollten auch bei jeder größeren Änderung der Infrastruktur, Prozesse oder Verfahren durchgeführt werden, die die Geschäftsfunktionen, Unterstützungsprozesse oder IT-Assets betreffen, und folglich sollte die aktuelle Risikobewertung der Finanzinstitute aktualisiert werden.

21. Die Finanzinstitute sollten sicherstellen, dass sie dauerhaft Gefahren und Schwachstellen in Bezug auf ihre Geschäftsfunktionen, Unterstützungsfunktionen und IT-Assets überwachen und die Risikoszenarien, die sie betreffen, regelmäßig überprüfen.

1.3.4. Risikominderung

22. Die Finanzinstitute sollten aufgrund von Risikobewertungen bestimmen, welche Maßnahmen erforderlich sind, um festgestellte IKT- und Sicherheitsrisiken auf akzeptable Niveaus zu verringern, und prüfen, ob Veränderungen an bestehenden Geschäftsprozessen, Kontrollmaßnahmen, IKT-Systemen und IKT-Diensten erforderlich sind. Das Finanzinstitut sollte die Umsetzungsdauer berücksichtigen, 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 Finanzinstituts zu bleiben.

23. Die Finanzinstitute sollten Maßnahmen zur Minderung von festgestellten IKT- und Sicherheitsrisiken und zum Schutz von IT-Assets in Übereinstimmung mit ihrer Klassifizierung festlegen und einführen.

1.3.5. Berichterstattung

24. Die Finanzinstitute sollten die Ergebnisse von Risikobewertungen klar und rechtzeitig an das Leitungsorgan berichten. Eine derartige Berichterstattung gilt unbeschadet der Verpflichtung von Zahlungsdienstleistern, den zuständigen Behörden eine aktualisierte und umfassende Risikobewertung gemäß Artikel 95 Absatz 2 der Richtlinie (EU) 2015/2366 vorzulegen.

1.3.6. Revision

25. Die Governance, Systeme sowie Prozesse für die IKT- und Sicherheitsrisiken eines Finanzinstituts müssen regelmäßig von Prüfern mit ausreichenden Kenntnissen, Fähigkeiten und ausreichendem Fachwissen im Bereich der IKT- und Sicherheitsrisiken sowie Zahlungsverkehr (für Zahlungsdienstleister) geprüft werden, um dem Leitungsorgan unabhängige Gewähr in Bezug auf die Wirksamkeit zu leisten. Die Prüfer sollten innerhalb des

Finanzinstituts oder vom Finanzinstitut unabhängig sein. Die Häufigkeit und der Schwerpunkt solcher Audits sollten den einschlägigen IKT- und Sicherheitsrisiken angemessen sein.

26. Das Leitungsorgan eines Finanzinstituts sollte den Prüfplan, einschließlich aller IKT-Audits und aller wesentlichen Änderungen dazu genehmigen. Der Auditplan und seine Ausführung, einschließlich der Häufigkeit der Audits, sollten die dazugehörenden IKT- und Sicherheitsrisiken im Finanzinstitut berücksichtigen und in einem angemessenen Verhältnis zu diesen stehen sowie regelmäßig aktualisiert werden.

27. Ein formeller Prozess zur Nachverfolgung, einschließlich Vorkehrungen für die rechtzeitige Überprüfung und Behebung kritischer Feststellungen der IKT-Prüfung sollte festgelegt werden.

1.4. Informationssicherheit

1.4.1. Informationssicherheitsleitlinie

28. Die Finanzinstitute sollten eine Informationssicherheitsleitlinie erarbeiten und dokumentieren, in der die übergeordneten Grundsätze und Regeln definiert, ausgearbeitet und dokumentiert werden, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Informationen der Finanzinstitute und ihrer Kunden zu schützen. Für Zahlungsdienstleister wird diese Leitlinie in dem gemäß Artikel 5 Absatz 1 Buchstabe j der Richtlinie (EU) 2015/2366 zu verabschiedeten Dokument zur Sicherheitsleitlinie festgelegt. Die Informationssicherheitsleitlinie sollte mit den Informationssicherheitszielen des Finanzinstituts übereinstimmen und auf den entsprechenden Ergebnissen des Risikobewertungsprozesses basieren. Die Leitlinie sollte vom Leitungsorgan genehmigt werden.

29. Die Leitlinie sollte eine Beschreibung der wichtigsten Rollen und Verantwortlichkeiten des Informationssicherheitsmanagements umfassen und die Anforderungen an das Personal und die Auftragnehmer, Prozesse und Technologie in Bezug auf die Informationssicherheit festlegen und dabei berücksichtigen, dass Mitarbeiter und Auftragnehmer auf allen Ebenen für die Gewährleistung der Informationssicherheit der Finanzinstitute verantwortlich sind. Die Leitlinie sollte die Vertraulichkeit, Integrität und Verfügbarkeit von kritischen, logischen und physischen IT-Assets, Ressourcen und sensiblen Daten sicherstellen, unabhängig davon, ob diese gespeichert, übertragen oder verwendet werden. Die Informationssicherheitsleitlinie sollte allen Mitarbeitern und Auftragnehmern des Finanzinstituts mitgeteilt werden.

30. Die Finanzinstitute sollten auf Grundlage der Informationssicherheitsleitlinie Sicherheitsmaßnahmen festlegen und einführen, um die IKT- und Sicherheitsrisiken zu mindern, denen sie ausgesetzt sind. Diese Maßnahmen sollten Folgendes umfassen:

    a) Organisation und Governance gemäß den Absätzen 10 und 11;
    b) logische Sicherheit (Abschnitt 3.4.2);
    c) physische Sicherheit (Abschnitt 3.4.3);
    d) IKT-Betriebssicherheit (Abschnitt 3.4.4);
    e) Sicherheitsüberwachung (Abschnitt 3.4.5);
    f) Überprüfung, Bewertung und Tests der Informationssicherheit (Abschnitt 3.4.6.);
    g) Schulung und Sensibilisierung hinsichtlich der Informationssicherheit (Abschnitt 3.4.7).

1.4.2. Logische Sicherheit

31. Die Finanzinstitute sollten Verfahren zur logischen Zugangskontrolle festlegen, dokumentieren und einführen (Identitäts- und Zugriffsmanagement). Diese Verfahren sollten eingeführt, durchgesetzt, überwacht und regelmäßig geprüft werden. Die Verfahren sollten auch Kontrollen für den Fall von Überwachungsanomalien umfassen. Mit diesen Verfahren sollten mindestens die folgenden Elemente eingeführt werden, wobei der Begriff „Nutzer“ auch technische Nutzer umfasst:

    (a) **„Need to know“- und „Least Privilege“-Prinzipien sowie Funktionstrennung**: Die Finanzinstitute sollten Zugriffsrechte auf IT-Assets und deren Unterstützungssysteme nach dem Grundsatz „Need to know“ verwalten, auch für den Fernzugang. Die Nutzer sollten nur jene Zugangsrechte erhalten, die zur Erfüllung ihrer Aufgaben unbedingt erforderlich sind (nach dem Grundsatz „Least Privilege“), d. h. um einen ungerechtfertigten Zugriff auf eine große Datenmenge zu verhindern oder die Zuweisung von Kombinationen von Zugriffsrechten, die zur Umgehung von Kontrollen verwendet werden können, zu verhindern (Grundsatz der „Funktionstrennung“).

    (b) **Eindeutige Zuordnung von Nutzern:** Die Finanzinstitute sollten die Verwendung allgemeiner und gemeinsamer Nutzerkonten so weit wie möglich einschränken und sicherstellen, dass die Nutzer für die in den IKT-Systemen durchgeführten Aktivitäten ermittelt werden können.

    (c) **Privilegierte Zugriffsrechte:** Die Finanzinstitute sollten strenge Kontrollen von privilegierten Systemzugriffen durchführen, indem sie die Anzahl der Konten mit erhöhten Systemzugangsrechten (z. B. Administratorkonten) begrenzen und genau überwachen. Um eine sichere Kommunikation zu gewährleisten und das Risiko zu reduzieren, sollte ein administrativer Fernzugriff auf kritische IKT-Systeme nur Personen gestattet werden, die Kenntnis über die entsprechenden Informationen haben müssen, und nur unter Anwendung von starken Authentifizierungslösungen erfolgen.

    (d) **Protokollierung von Nutzeraktivitäten:** Zumindest sollten alle Aktivitäten von privilegierten Nutzern protokolliert und überwacht werden. Zugriffsprotokolle sollten im Einklang mit Abschnitt 3.3.3 unbeschadet der im EU-Recht und im nationalen Recht festgelegten Aufbewahrungsanforderungen gesichert werden, vor unbefugten Änderungen oder Löschungen geschützt und für einen Zeitraum aufbewahrt werden, welcher der Kritikalität der ermittelten Geschäftsfunktionen, Unterstützungsprozesse und IT-Assets angemessen ist. Das Finanzinstitut sollte diese Informationen nutzen, um die Identifizierung und Untersuchung ungewöhnlicher Aktivitäten, die bei der Erbringung von Diensten festgestellt wurden, zu erleichtern.

    (e) **Zugriffsmanagement:** Zugriffsrechte sollten gemäß vordefinierten Genehmigungsabläufen, an denen der Eigentümer der Informationen, auf die zugegriffen wird (Eigentümer der Informationen), beteiligt ist, rechtzeitig gewährt, entzogen oder geändert werden. Für den Fall einer Beendigung des Beschäftigungsverhältnisses sollten die Zugriffsrechte unverzüglich entzogen werden.

(f) **Rezertifizierung des Zugriffs**: Die Zugriffsrechte sollten regelmäßig überprüft werden, um sicherzustellen, dass die Nutzer keine übermäßigen Rechte besitzen und dass die Zugriffsrechte entzogen werden, wenn sie nicht mehr benötigt werden.

(g) **Authentifizierungsmethoden:** Die Finanzinstitute sollten Authentifizierungsmethoden einführen, die stark genug sind, um auf angemessene und wirksame Weise sicherzustellen, dass die Regelungen und Verfahren in Bezug auf Zugriffsrechte befolgt werden. Authentifizierungsmethoden sollten der Kritikalität der IKT-Systeme, der IKT-Informationen oder des Zugriffsprozesses angemessen sein. Dies sollte auf Grundlage des jeweiligen Risikos zumindest komplexe Passwörter oder stärkere Authentifizierungsmethoden (wie z. B. Zwei-Faktor-Authentifizierung) umfassen.

32. Der elektronische Zugriff auf Daten und IKT-Systeme durch Anwendungen sollte auf ein für die Erbringung der relevanten Dienstleistung erforderliches Mindestmaß beschränkt werden.

1.4.3. Physische Sicherheit

33. Zum Schutz der Räumlichkeiten, Rechenzentren und sensiblen Bereiche der Finanzinstitute vor unbefugtem Zugriff und elementaren Gefahren sollten physische Sicherheitsmaßnahmen der Finanzinstitute festgelegt, dokumentiert und umgesetzt werden.

34. Der physische Zugriff auf IKT-Systeme sollte nur berechtigten Personen gestattet sein. Die Berechtigung sollte in Übereinstimmung mit den Aufgaben und Verantwortlichkeiten Einzelner erteilt und auf Personen beschränkt werden, die entsprechend geschult wurden und beaufsichtigt werden. Der physische Zugriff sollte regelmäßig überprüft werden, um sicherzustellen, dass nicht erforderliche Zugriffsrechte sofort zurückgezogen werden, sobald sie nicht mehr erforderlich sind.

35. Die Schutzmaßnahmen gegenüber Elementarereignissen sollten der Bedeutung der Gebäude und der Kritikalität der Tätigkeiten oder der in diesen Gebäuden beherbergten IKT-Systeme angemessen sein.

1.4.4. Sicherer Betrieb von IKT

36. Die Finanzinstitute sollten Verfahren einführen, um das Auftreten von Sicherheitsproblemen bei IKT-Systemen und IKT-Diensten zu vermeiden und ihre Auswirkungen auf die Erbringung von IKT-Diensten zu minimieren. Diese Verfahren sollten die folgenden Maßnahmen umfassen:

a) Durch die Identifizierung und Bewertung von möglichen Schwachstellen sollte durch Einspielen von kritischen Sicherheitspatches oder durch alternative Maßnahmen sichergestellt werden, dass Software und Firmware auf dem neuesten Stand sind. Dies gilt auch für Software, welche die Finanzinstitute ihren internen und externen Nutzern zur Verfügung stellen;

b) Implementierung sicherer Konfigurationsbaselines aller Netzwerkkomponenten;

c) Einführung einer Netzwerksegmentierung, von Systemen zur Vermeidung von Datenverlusten und Verschlüsselung des Netzverkehrs (entsprechend der Datenklassifizierung);

d) Einführung von Endgerätesicherheit, einschließlich Servern, Arbeitsplätzen und mobilen Geräten; die Finanzinstitute sollten bewerten, ob die Endgeräte die von ihnen festgelegten Sicherheitsstandards erfüllen, bevor ihnen der Zugriff zum Unternehmensnetzwerk gewährt wird;
e) Gewährleistung des Vorhandenseins von Mechanismen zur Überprüfung der Integrität von Software, Firmware und Daten;
f) Verschlüsselung von Daten bei Speicherung und Übertragung (gemäß der Datenklassifizierung).

37. Des Weiteren sollten die Finanzinstitute laufend feststellen, ob Änderungen der bestehenden Betriebsumgebung Auswirkungen auf die bestehenden Sicherheitsmaßnahmen haben oder zusätzliche Maßnahmen zur Minderung betreffender Risiken erforderlich machen. Diese Änderungen sollten einen Teil des formalen Änderungsmanagementprozesses der Finanzinstitute darstellen, durch den sichergestellt werden sollte, dass alle Änderungen ordnungsgemäß geplant, getestet, dokumentiert, autorisiert und umgesetzt werden.

1.4.5. Überwachung der IKT- und Informationssicherheit

38. Die Finanzinstitute sollten Regelungen und Verfahren erstellen und einführen, um ungewöhnliche Aktivitäten zu identifizieren, welche die Informationssicherheit der Finanzinstitute beeinflussen könnten, und um auf diese Ereignisse auf angemessene Weise reagieren zu können. Im Rahmen dieser kontinuierlichen Überwachung sollten die Finanzinstitute angemessene und effektive Funktionen zur Erkennung und Meldung des physischen oder logischen Eindringens sowie zur Erkennung von Verstößen gegen die Vorschriften bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit der IT-Assets einführen. Die kontinuierlichen Überwachungs- und Erkennungsprozesse sollten Folgendes umfassen:

a) relevante interne und externe Faktoren, einschließlich Geschäfts- und IKT-Administrationsfunktionen;
b) Transaktionen zur Erkennung eines Missbrauchs des Zugriffs durch Dritte oder andere Organisationen und eines internen Missbrauchs des Zugriffs;
c) potenzielle interne und externe Gefahren.

39. Die Finanzinstitute sollten Prozesse und Organisationsstrukturen einrichten und implementieren, um sicherheitsrelevante Gefahren, die ihre Fähigkeiten zur Erbringung von Dienstleistungen wesentlich beeinträchtigen könnten, zu ermitteln und ständig zu überwachen. Die Finanzinstitute sollten technologische Entwicklungen aktiv überwachen, um sicherzustellen, dass sie Kenntnis von sicherheitsrelevanten Risiken haben. Die Finanzinstitute sollten Erkennungsmaßnahmen einführen, zum Beispiel zur Feststellung möglicher Datenlecks, eines schädlichen Codes und sonstiger Sicherheitsrisiken sowie von öffentlich bekannten Schwachstellen in der Software und Hardware, und entsprechende neue Sicherheitsupdates ermitteln.

40. Der Sicherheitsüberwachungsprozess sollte einem Finanzinstitut auch dabei helfen, die Art der Betriebs- und Sicherheitsvorfälle zu verstehen, Trends zu erkennen und die Untersuchungen der Organisation zu unterstützen.

1.4.6. Überprüfungen, Bewertungen und Tests der Informationssicherheit

41. Die Finanzinstitute sollten eine Vielzahl von Überprüfungen, Bewertungen und Tests in Bezug auf die Informationssicherheit durchführen, um die wirksame Ermittlung von Schwachstellen in ihren IKT-Systemen und IKT-Diensten sicherzustellen. So können Finanzinstitute Gap-Analysen anhand von Informationssicherheitsstandards, Konformitätsprüfungen, interne und externe Prüfungen der Informationssysteme oder Überprüfungen der physischen Sicherheit durchführen. Zudem sollte das Institut bewährte Verfahren wie Quellcode-Überprüfungen, Schwachstellenmanagement, Penetrationstests und Simulationen von Angriffen (Red-Team-Tests) erwägen.

42. Die Finanzinstitute sollten ein Rahmenwerk für Informationssicherheitstests schaffen und implementieren, um die Robustheit und Wirksamkeit ihrer Informationssicherheitsmaßnahmen zu bewerten, und sicherzustellen, dass dieser Rahmen Bedrohungen und Verwundbarkeiten berücksichtigt, die durch die Bedrohungsüberwachung und den Informationsrisikomanagementprozess ermittelt werden.

43. Das Rahmenwerk für Tests der Informationssicherheit sollte sicherstellen, dass die Tests:

    a) von unabhängigen Prüfern durchgeführt werden, die über ausreichende Kenntnisse, Fähigkeiten und ausreichendes Fachwissen im Bereich der Prüfung von Informationssicherheitsmaßnahmen verfügen und nicht an der Entwicklung der Informationssicherheitsmaßnahmen beteiligt sind;
    b) Schwachstellen- und Penetrationstests (einschließlich Bedrohungs-Penetrationstests, falls erforderlich und angemessen) umfassen, die dem mit den Geschäftsprozessen und -systemen ermittelten Risikoniveau entsprechen.

44. Die Finanzinstitute sollten laufende und wiederholte Tests in Bezug auf die Sicherheitsmaßnahmen durchführen. Für alle kritischen IKT-Systeme (Absatz 17) sollten diese Tests mindestens einmal jährlich durchgeführt werden und für Zahlungsdienstleister gemäß Artikel 95 Absatz 2 der PSD2 Teil der umfassenden Bewertung der Sicherheitsrisiken im Zusammenhang mit den von ihnen erbrachten Zahlungsdiensten sein. Nicht kritische Systeme sollten regelmäßig unter Verwendung eines risikobasierten Ansatzes, jedoch mindestens alle drei Jahre geprüft werden.

45. Die Finanzinstitute sollten sicherstellen, dass Tests der Sicherheitsmaßnahmen bei Änderungen der Infrastruktur, Prozesse oder Verfahren sowie bei Änderungen aufgrund großer Betriebs- oder Sicherheitsvorfälle oder bei der Freigabe neuer oder in großen Umfang geänderter internetbezogener kritischer Anwendungen durchgeführt werden.

46. Die Finanzinstitute sollten die Ergebnisse der Sicherheitstests überwachen, auswerten und Sicherheitsmaßnahmen entsprechend anpassen. Im Falle kritischer IKT-Systeme sind die Sicherheitsmaßnahmen unverzüglich anzupassen.

47. Für Zahlungsdienstleister sollte die Testumgebung zudem die Sicherheitsmaßnahmen umfassen, die für (1) Zahlungsterminals und -geräte, die für die Erbringung von Zahlungsdiensten verwendet werden, (2) Zahlungsterminals und -geräte, die für die Authentifizierung der Zahlungsdienstnutzer verwendet werden, und (3) Geräte und Software,

die ein Zahlungsdienstleister dem Zahlungsdienstnutzer zur Verfügung stellt, um einen Authentifizierungscode zu generieren/erhalten, relevant sind.

48. Auf Grundlage der festgestellten Sicherheitsbedrohungen und der vorgenommenen Änderungen sollten Tests durchgeführt werden, um Szenarien bezüglich relevanter und bekannter potenzieller Angriffe einzubeziehen.

1.4.7. Informationssicherheitsschulung und -sensibilisierung

49. Die Finanzinstitute sollten ein Schulungsprogramm, einschließlich periodischer Sensibilisierungsprogramme für alle Mitarbeiter und Auftragnehmer einrichten, um sicherzustellen, dass diese für die Durchführung ihrer Aufgaben und Verantwortlichkeiten, sowie im Umgang mit Informationssicherheitsrisiken, in Übereinstimmung mit den einschlägigen Informationssicherheitsleitlinien und -verfahren geschult sind, sodass menschliche Fehler, Diebstahl, Betrug, Missbrauch oder Verlust reduziert werden. Die Finanzinstitute sollten sicherstellen, dass das Schulungsprogramm für alle Mitarbeiter und Auftragnehmer mindestens einmal jährlich eine Schulung vorsieht.

1.5. IKT-Betriebsmanagement

50. Die Finanzinstitute sollten ihre IKT-Tätigkeiten auf der Grundlage, vom Leitungsorgan genehmigten, dokumentierter und eingeführter Prozesse (die für Zahlungsdienstleister das Dokument zur Sicherheitsstrategie gemäß Artikel 5 Absatz 1 Buchstabe j der PSD2 umfassen) steuern. In den Dokumenten sollte festgelegt werden, wie Finanzinstitute ihre IKT-Systeme und -dienste betreiben, überwachen und kontrollieren, einschließlich der Dokumentation kritischer IKT-Tätigkeiten, und die Finanzinstitute in die Lage versetzen, ihr IKT-Systeminventar ständig auf aktuellem Stand zu halten.

51. Die Finanzinstitute sollten sicherstellen, dass die Leistung ihrer IKT-Tätigkeiten im Einklang mit ihren Geschäftsanforderungen steht. Die Finanzinstitute sollten die Effizienz ihrer IKT-Tätigkeiten aufrechterhalten und nach Möglichkeit verbessern, wobei sie insbesondere prüfen sollten, wie potenzielle Fehler, die sich aus der Durchführung manueller Aufgaben ergeben, minimiert werden können.

52. Die Finanzinstitute sollten Protokollierungs- und Überwachungsverfahren für kritische IKT-Tätigkeiten einführen, um die Erkennung, Analyse und Korrektur von Fehlern zu ermöglichen.

53. Die Finanzinstitute sollten ein aktuelles Verzeichnis ihrer IKT-Assets (einschließlich IKT-Systeme, Netzwerkgeräte, Datenbanken usw.) führen. Das IKT-Systeminventar sollte die Konfiguration der IKT-Systeme sowie die Verbindungen und Abhängigkeiten zwischen den verschiedenen IKT-Systemen enthalten, um einen ordnungsgemäßen Konfigurations- und Änderungsmanagementprozess zu ermöglichen.

54. Das IKT-Systeminventar sollte hinreichend detailliert sein, um die sofortige Identifizierung eines IKT-Systems, seines Standorts, seiner Sicherheitsklassifizierung und seiner Eigentümerschaft zu ermöglichen. Die Abhängigkeiten zwischen den Systemen sollten zur Unterstützung bei der

Reaktion auf Sicherheits- und Betriebsvorfälle, einschließlich Cyberangriffen, dokumentiert werden.

55. Die Finanzinstitute sollten die Lebenszyklen von IKT-Systemen überwachen und verwalten, um zu gewährleisten, dass diese weiterhin die Anforderungen des Geschäfts- und Risikomanagements erfüllen und unterstützen. Die Finanzinstitute sollten überwachen, ob ihre IKT-Systeme von ihren externen oder internen Anbietern und Entwicklern unterstützt werden und ob alle relevanten Patches und Upgrades auf der Basis dokumentierter Prozesse angewendet werden. Die Risiken aufgrund veralteter oder nicht unterstützter IKT-Systeme sollten bewertet und gemindert werden.

56. Die Finanzinstitute sollten Leistungs- und Kapazitätsplanungs- und -überwachungsprozesse einführen, um bedeutende Leistungsprobleme von IKT-Systemen und Engpässe bei IKT-Kapazitäten rechtzeitig zu verhindern, aufzudecken und darauf zu reagieren.

57. Die Finanzinstitute sollten Verfahren zur Sicherung und Wiederherstellung von Daten und IKT-Systemen festlegen und einführen, um sicherzustellen, dass sie bei Bedarf wiederhergestellt werden können. Umfang und Häufigkeit von Back-ups sollten im Einklang mit den Anforderungen an die Wiederherstellung des Geschäftsbetriebs und der Kritikalität der Daten und IKT-Systeme festgelegt und entsprechend der durchgeführten Risikobewertung beurteilt werden. Die Backup- und Wiederherstellungsverfahren sollten regelmäßig getestet werden.

58. Die Finanzinstitute sollten sicherstellen, dass Daten- und IKT-System-Backups sicher gespeichert werden und sich in einer ausreichenden Entfernung vom Primärstandort befinden, so dass sie nicht denselben Risiken ausgesetzt sind.

3.5.1 IKT-Vorfalls- und Problemmanagement

59. Die Finanzinstitute sollten einen Prozess zum Management von Vorfällen und Problemen einrichten und umsetzen, um operationelle und sicherheitsrelevante IKT-Vorfälle zu überwachen und zu protokollieren und es den Finanzinstituten zu ermöglichen, kritische Geschäftsfunktionen und -prozesse bei Störungen zeitnah fortzuführen oder wiederaufzunehmen. Die Finanzinstitute sollten geeignete Kriterien und Grenzwerte für die Einstufung von Vorfällen als Betriebs- oder Sicherheitsvorfälle gemäß der Definition im Abschnitt „Begriffsbestimmungen“ sowie Frühwarnindikatoren festlegen, die als Warnungen für die frühzeitige Erkennung dieser Vorfälle dienen. Diese Kriterien und Schwellenwerte für Zahlungsdienstleister gelten unbeschadet der Einstufung von schwerwiegenden Vorfällen gemäß Artikel 96 der PSD2 und den Leitlinien für die Meldung schwerwiegender Vorfälle gemäß der PSD2 (EBA/GL/2017/10).

60. Um die Auswirkungen negativer Ereignisse so gering wie möglich zu halten und eine rechtzeitige Wiederherstellung zu ermöglichen, sollten die Finanzinstitute geeignete Verfahren und Organisationsstrukturen schaffen, um eine kohärente und integrierte Überwachung, Bearbeitung und Weiterverfolgung von Betriebs- und Sicherheitsvorfällen zu gewährleisten und sicherzustellen, dass die Hauptursachen ermittelt und beseitigt werden, um eine Wiederholung

der Vorfälle zu vermeiden. Der Vorfall- und Problemmanagementprozess sollte Folgendes umfassen:

a) je nach Geschäftskritikalität Verfahren zur Ermittlung, Verfolgung, Protokollierung, Kategorisierung und Einstufung von Sicherheitsvorfällen nach Prioritäten;
b) Rollen und Zuständigkeiten für verschiedene Ereignisszenarien (z. B. Fehler, Funktionsstörungen, Cyberangriffe);
c) Problemmanagementverfahren zur Ermittlung, Analyse und Lösung der Hauptursache eines oder mehrerer Vorfälle – das Finanzinstitut sollte die Betriebs- oder Sicherheitsvorfälle analysieren, die das Finanzinstitut betreffen könnten und die innerhalb und/oder außerhalb der Organisation festgestellt wurden oder aufgetreten sind, und die wichtigsten Erkenntnisse aus diesen Analysen berücksichtigen und die Sicherheitsmaßnahmen entsprechend aktualisieren;
d) wirksame interne Kommunikationspläne, einschließlich der Meldung von Vorfällen und Eskalationsverfahren - einschließlich sicherheitsrelevante Kundenbeschwerden -, um sicherzustellen, dass
    i) Vorfälle mit potenziell hohen negativen Auswirkungen auf kritische IKT-Systeme und IKT-Dienste der zuständigen Geschäftsleitung und der Leitung der IKT-Abteilung gemeldet werden;
    ii) das Leitungsorgan bei bedeutenden Vorfällen auf Ad-hoc-Basis informiert wird, zumindest über die Auswirkungen, die Reaktion und die zusätzlichen Kontrollen, die als Folge der Vorfälle festzulegen sind.
e) Verfahren zur Reaktion auf Vorfälle, um die Auswirkungen der Vorfälle zu mindern und sicherzustellen, dass der Dienst rechtzeitig betriebsbereit und sicher ist;
f) spezifische externe Kommunikationspläne für kritische Geschäftsfunktionen und -prozesse, um
    i) mit relevanten Akteuren zusammenzuarbeiten, damit wirksam auf den Vorfall reagiert und dieser behoben werden kann;
    ii) ggf. externe Beteiligte (z. B. Kunden, andere Marktteilnehmer, die Aufsichtsbehörde) im Einklang mit einer geltenden Verordnung rechtzeitig zu informieren.

1.6. IKT-Projekt- und Änderungsmanagement

1.6.1. IKT-Projektmanagement

61. Das Finanzinstitut sollte eine Programm- und/oder eine Projekt-Governance einführen, mit der Aufgaben, Zuständigkeiten und Verantwortlichkeiten festgelegt werden, um die Umsetzung der IKT-Strategie wirksam zu unterstützen.

62. Das Finanzinstitut sollte Risiken, die sich aus seinem Portfolio von IKT-Projekten (Programmmanagement) ergeben, angemessen überwachen und mindern, wobei auch Risiken zu berücksichtigen sind, die sich aus Abhängigkeiten zwischen verschiedenen Projekten und aus Abhängigkeiten mehrerer Projekte von denselben Ressourcen und/oder demselben Fachwissen ergeben können.

63. Das Finanzinstitut sollte Vorgaben für das IKT-Projektmanagement festlegen und umsetzen, die mindestens Folgendes umfassen:

    a) Projektziele;
    b) Rollen und Verantwortlichkeiten;
    c) eine Projektrisikobewertung;
    d) einen Plan, Zeitrahmen sowie die Schritte des Projekts;
    e) wichtige Meilensteine;
    f) Anforderungen an das Änderungsmanagement.

64. Die Vorgaben zum IKT-Projektmanagement sollten sicherstellen, dass die Anforderungen an die Informationssicherheit von einer Funktion geprüft und genehmigt werden, die von der Entwicklungsfunktion unabhängig ist.

65. Das Finanzinstitut sollte sicherstellen, dass alle von einem IKT-Projekt betroffenen Bereiche im Projektteam vertreten sind und dass das Projektteam über die für eine sichere und erfolgreiche Projektdurchführung erforderlichen Kenntnisse verfügt.

66. Die Einrichtung und der Fortschritt von IKT-Projekten und die damit verbundenen Risiken sollten dem Leitungsorgan je nach Bedeutung und Umfang der IKT-Projekte einzeln oder zusammenfassend, regelmäßig und gegebenenfalls auf Ad-hoc-Basis gemeldet werden. Die Finanzinstitute sollten das Projektrisiko im Rahmen ihres Risikomanagementrahmens einbeziehen.

1.6.2. Erwerb und Entwicklung von IKT-Systemen

67. Die Finanzinstitute sollten einen Prozess für den Erwerb, die Entwicklung und die Wartung von IKT-Systemen entwickeln und einführen. Dieser Prozess sollte einen risikobasierten Ansatz berücksichtigen.

68. Das Finanzinstitut sollte dafür Sorge tragen, dass vor dem Erwerb oder der Entwicklung von IKT-Systemen die funktionalen und nichtfunktionalen Anforderungen (einschließlich Anforderungen an die Informationssicherheit) von der zuständigen Geschäftsleitung klar festgelegt und genehmigt werden.

69. Das Finanzinstitut sollte dafür Sorge tragen, dass Maßnahmen ergriffen werden, um das Risiko einer unbeabsichtigten Änderung oder absichtlichen Manipulation der IKT-Systeme während der Entwicklung und Implementierung in der Produktionsumgebung zu verringern.

70. Die Finanzinstitute sollten über eine Methodik zur Überprüfung und Genehmigung von IKT-Systemen vor ihrer ersten Nutzung verfügen. Diese Methodik sollte die Kritikalität von Geschäftsprozessen und Vermögenswerten berücksichtigen. Die Tests sollten sicherstellen, dass neue IKT-Systeme die beabsichtigte Leistung erbringen. Sie sollten auch Testumgebungen verwenden, die die Produktionsumgebung angemessen wiedergeben.

71. Die Finanzinstitute sollten IKT-Systeme, IKT-Dienste und Maßnahmen zur Informationssicherheit testen, um potenzielle Sicherheitsschwächen, -verletzungen und -vorfälle zu ermitteln.

72. Das Finanzinstitut sollte getrennte IKT-Umgebungen implementieren, um eine ausreichende Funktionstrennung zu gewährleisten und um die Auswirkungen von nichtverifizierten Änderungen an den Produktionssystemen zu verhindern. Im Besonderen sollte das Finanzinstitut die Trennung der Produktionsumgebung von den Entwicklungs-, Test- und anderen Nicht-Produktionsumgebungen gewährleisten. Das Finanzinstitut sollte die Integrität und Vertraulichkeit von Produktivdaten in Nicht- Produktionsumgebungen sicherstellen. Der Zugang zu Produktionsdaten ist auf autorisierte Nutzer beschränkt.

73. Die Finanzinstitute sollten Maßnahmen zum Schutz der Integrität der Quellcodes von intern entwickelten IKT-Systemen implementieren. Ferner sollten sie die Entwicklung, Implementierung, den Betrieb und/oder die Konfiguration der IKT-Systeme umfangreich dokumentieren, um eine unnötige Abhängigkeit von Fachexperten zu reduzieren. Die Dokumentation des IKT-Systems sollte zumindest eine Benutzerdokumentation, eine technische Systemdokumentation und eine Beschreibung der Betriebsabläufe enthalten.

74. Die Verfahren eines Finanzinstituts für den Erwerb und die Entwicklung von IKT-Systemen sollten auch für IKT-Systeme gelten, die von den Endnutzern der Geschäftsfunktion unter Verwendung eines risikobasierten Ansatzes außerhalb der IKT-Organisation entwickelt oder verwaltet werden (z. B. Endnutzer-Computeranwendungen). Das Finanzinstitut sollte ein Register dieser Anwendungen führen, die kritische Geschäftsfunktionen oder -prozesse unterstützen.

1.6.3. IKT-Änderungsmanagement

75. Die Finanzinstitute sollten ein Prozess für das IKT-Änderungsmanagement einrichten, um sicherzustellen, dass alle Änderungen an IKT-Systemen auf kontrollierte Weise erfasst, getestet, bewertet, genehmigt, umgesetzt und überprüft werden. Die Finanzinstitute sollten die Notfalländerungen (d. h. Änderungen, die so schnell wie möglich eingeführt werden müssen) nach Verfahren durchführen, die angemessene Sicherheitsstandards bieten.

76. Die Finanzinstitute sollten fortlaufend feststellen, ob Änderungen der bestehenden Betriebsumgebung Auswirkungen auf die bestehenden Sicherheitsmaßnahmen haben oder zusätzliche Maßnahmen zur Minderung der betreffenden Risiken erforderlich machen. Diese Änderungen sollten im Einklang mit dem formalen Änderungsmanagementprozess der Finanzinstitute stehen.

1.7. Geschäftsfortführungsmanagement

77. Die Finanzinstitute sollten ein solides Geschäftsfortführungsmanagement (BCM) einrichten, um ihre Fähigkeit zur kontinuierlichen Erbringung von Dienstleistungen zu maximieren und Verluste im Falle einer schwerwiegenden Betriebsunterbrechung gemäß Artikel 85 Absatz 2 der Richtlinie 2013/36/EU und Titel VI der EBA-Leitlinien zur internen Governance (EBA/GL/2017/11) zu begrenzen.

1.7.1. Business-Impact-Analyse (BIA)

78. Als Teil eines soliden Geschäftsfortführungsmanagements sollten die Finanzinstitute eine Analyse der Auswirkungen auf das Unternehmen durchführen, indem sie ihre Gefährdung durch schwerwiegende Betriebsunterbrechungen analysieren und deren potenzielle Auswirkungen (einschließlich der Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit) quantitativ und qualitativ bewerten, wobei sie interne und/oder externe Daten (z. B. Daten von Drittanbietern, die für einen Geschäftsprozess relevant sind, oder öffentlich verfügbare Daten, die für die BIA relevant sein können) und Szenarioanalysen verwenden. Die BIA sollte auch die Kritikalität der festgestellten und klassifizierten Geschäftsfunktionen, der Unterstützungsprozesse, von Dritten und der IT-Assets sowie deren Abhängigkeiten gemäß Abschnitt 3.3.3 berücksichtigen.

79. Die Finanzinstitute sollten sicherstellen, dass ihre IKT-Systeme und IKT-Dienste so konzipiert und auf ihre BIA abgestimmt sind, dass beispielsweise bestimmte kritische Komponenten redundant ausgelegt sind, um Störungen durch Ereignisse mit Auswirkungen auf diese Komponenten zu verhindern.

1.7.2. Geschäftsfortführungsplanung

80. Auf Grundlage ihrer BIA sollten die Finanzinstitute Pläne zur Gewährleistung der Kontinuität des Geschäftsbetriebs (Geschäftsfortführungspläne, BCPs) aufstellen, die von ihren Leitungsorganen dokumentiert und genehmigt werden sollten. In den Plänen sollten insbesondere Risiken berücksichtigt werden, die sich nachteilig auf IKT-Systeme und IKT-Dienste auswirken könnten. Die Pläne sollten den Schutz und gegebenenfalls die Wiederherstellung des Vertrauens, der Integrität und der Verfügbarkeit ihrer Geschäftsfunktionen, Unterstützungsprozesse und IT-Assets unterstützen. Die Finanzinstitute sollten sich bei der Erstellung dieser Pläne gegebenenfalls mit den relevanten internen und externen Akteuren abstimmen.

81. Die Finanzinstitute sollten BCPs einrichten, um sicherzustellen, dass sie auf potenzielle Ausfallszenarien angemessen reagieren können und in der Lage sind, den Betrieb ihrer kritischen Geschäftstätigkeiten nach Störungen innerhalb einer vorgegebenen Wiederherstellungszeit („recovery time objective“, RTO, maximale Zeitspanne, innerhalb der ein System oder Prozess nach einem Vorfall wiederhergestellt werden muss) und zu einem vorgegebenen Wiederherstellungspunkt („recovery point objective“, RPO, maximale Zeitspanne, innerhalb derer ein Datenverlust bei einem Vorfall akzeptabel ist) wiederherzustellen. Bei schwerwiegenden Betriebsunterbrechungen, die spezielle Geschäftsfortführungspläne auslösen, sollten die Finanzinstitute Prioritäten bei den Geschäftsfortführungsmaßnahmen festlegen, wobei sie einen risikobasierten Ansatz verfolgen, der sich auf die gemäß Abschnitt 3.3.3 durchgeführten Risikobewertungen stützen kann. Für Zahlungsdienstleister kann dies beispielsweise die Ermöglichung der weiteren Verarbeitung kritischer Transaktionen bei gleichzeitiger Fortsetzung der Wiederherstellungsbemühungen beinhalten.

82. Das Finanzinstitut sollte eine Reihe verschiedener Szenarien in seinem BCP berücksichtigen, einschließlich extremer, jedoch denkbarer Szenarien, denen es ausgesetzt sein kann, einschließlich eines Cyberangriffsszenarios, und es sollte die möglichen Auswirkungen dieser Szenarien bewerten. Ausgehend von diesen Szenarien sollte das Finanzinstitut beschreiben, wie die Kontinuität der IKT-Systeme und -Dienste sowie die Informationssicherheit des Finanzinstituts gewährleistet werden.

1.7.3. Reaktions- und Wiederherstellungspläne

83. Aufgrund der BIAs (Absatz 78) und möglichen Szenarien (Absatz 82) sollten die Finanzinstitute Reaktions- und Wiederherstellungspläne ausarbeiten. In diesen Plänen sollte festgelegt werden, unter welchen Bedingungen die Pläne aktiviert werden können und welche Maßnahmen ergriffen werden sollten, um die Verfügbarkeit, Kontinuität und Wiederherstellung zumindest der kritischen IKT-Systeme und IKT-Dienste von Finanzinstituten zu gewährleisten. Mit den Reaktions- und Wiederherstellungsplänen sollten die Wiederherstellungsziele der Finanzinstitute erreicht werden.

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

    a) sich auf die Wiederherstellung der Geschäftstätigkeit kritischer Geschäftsfunktionen, Unterstützungsprozesse, IT-Assets und deren wechselseitige Abhängigkeiten zur Vermeidung nachteiliger Auswirkungen auf die Funktionsweise von Finanzinstituten und auf das Finanzsystem, einschließlich Zahlungssysteme und Zahlungsdienstnutzer, beziehen und die Ausführung ausstehender Zahlungsvorgänge gewährleisten;
    b) dokumentiert werden und den Geschäfts- und Unterstützungseinheiten zur Verfügung gestellt werden und im Notfall leicht zugänglich sein;
    c) İn Übereinstimmung mit den Erfahrungen aus Vorfällen, Tests, ermittelten neuen Risiken und Bedrohungen sowie geänderten Wiederherstellungszielen und -prioritäten aktualisiert werden.

85. Die Pläne sollten auch alternative Optionen berücksichtigen, bei denen eine Wiederherstellung aufgrund von Kosten, Risiken, Logistik oder unvorhergesehenen Umständen kurzfristig nicht möglich ist.

86. Darüber hinaus sollte das Finanzinstitut im Rahmen der Reaktions- und Wiederherstellungspläne Maßnahmen zur Gewährleistung der Kontinuität erwägen und einführen, um Ausfälle von Drittanbietern zu mildern, die für die Kontinuität der IKT-Dienste eines Finanzinstituts von entscheidender Bedeutung sind (im Einklang mit den Bestimmungen der EBA-Leitlinien zu Auslagerungen (EBA/GL/2019/02) in Bezug auf Geschäftsfortführungspläne).

1.7.4. Testen von Plänen

87. Die Finanzinstitute sollten ihre BCPs regelmäßig testen. Sie sollten insbesondere sicherstellen, dass die BCPs ihrer kritischen Geschäftsfunktionen, Unterstützungsprozesse, IT-Assets und ihre wechselseitigen Abhängigkeiten (gegebenenfalls auch die von Dritten) mindestens einmal jährlich gemäß Absatz 89 geprüft werden.

88. BCPs sollten mindestens einmal jährlich auf der Grundlage von Testergebnissen, aktuellen Erkenntnissen über Bedrohungen und Erfahrungen aus früheren Ereignissen aktualisiert werden. Etwaige Änderungen der Wiederherstellungsziele (einschließlich RTO und RPO) und/oder Änderungen der Geschäftsfunktionen, der Unterstützungsprozesse und der IT-Assets sollten gegebenenfalls auch als Grundlage für die Aktualisierung der BCPs berücksichtigt werden.

89. Die Prüfung der BCPs durch Finanzinstitute sollte nachweisen, dass sie die Funktionsfähigkeit ihrer Geschäfte bis zur Wiederherstellung kritischer Operationen aufrechterhalten können. Insbesondere sollten sie:

    a) die Prüfung angemessen schwerer, aber plausibler Szenarien, einschließlich der für die Entwicklung der BCPs in Betracht gezogenen Szenarien (sowie gegebenenfalls die Prüfung von Diensten, die von Dritten erbracht werden) umfassen; dies sollte die Umstellung kritischer Geschäftsfunktionen, Unterstützungsprozesse und IT-Assets für die Notfallwiederherstellungsumgebung und den Nachweis umfassen, dass sie auf diese Weise für einen ausreichend repräsentativen Zeitraum betrieben werden können und dass die normale Funktion danach wiederhergestellt werden kann;
    b) die Prüfung so gestalten, dass die Annahmen, auf die sich die Geschäftsfortführungspläne im Krisenfall stützen, einschließlich der Governance-Regelungen und der Krisenkommunikationspläne, hinterfragt werden; und
    c) Verfahren zur Überprüfung der Fähigkeit ihres Personals und ihrer Auftragnehmer, der IKT-Systeme und IKT-Dienste, auf die in Ziffer 89 Buchstabe a definierten Szenarien angemessen zu reagieren, umfassen.

90. Die Testergebnisse sollten dokumentiert werden und alle aus den Tests resultierenden festgestellten Mängel sollten analysiert, behandelt und dem Leitungsorgan gemeldet werden.

1.7.5. Krisenkommunikation

91. Bei einer Störung oder einem Notfall und während der Umsetzung von BCPs im Krisenfall sollten die Finanzinstitute sicherstellen, dass sie wirksame Maßnahmen zur Krisenkommunikation eingeführt haben, so dass alle relevanten internen und externen Akteure, einschließlich der zuständigen Behörden, wenn dies in den nationalen Rechtsvorschriften vorgeschrieben ist, sowie einschlägiger Anbieter (Outsourcing-Anbieter, Gruppenunternehmen oder Drittanbieter) rechtzeitig und angemessen informiert werden.

1.8. Pflege der Kundenbeziehungen mit Zahlungsdienstnutzern

92. Die Zahlungsdienstleister sollten Prozesse einrichten und implementieren, durch die das Bewusstsein der Zahlungsdienstnutzer über die sicherheitsrelevanten Risiken in Bezug auf die Zahlungsdienste verbessert wird, indem die Zahlungsdienstnutzer unterstützt und beraten werden.

93. Die den Zahlungsdienstnutzern angebotene Unterstützung und Beratung sollte im Hinblick auf neue Gefahren und Schwachstellen aktualisiert werden, und Änderungen sollten den Zahlungsdienstnutzern mitgeteilt werden.

94. Wenn die Produktfunktionalität dies zulässt, sollten die Zahlungsdienstleister den Zahlungsdienstnutzern gestatten, bestimmte Zahlungsfunktionen in Verbindung mit den Zahlungsdiensten, die die Zahlungsdienstleister den Zahlungsdienstnutzern anbieten, zu deaktivieren.

95. Wenn der Zahlungsdienstleister gemäß Artikel 68 Absatz 1 der Richtlinie (EU) 2015/2366 Ausgabenobergrenzen für Zahlungsvorgänge, die durch dieses Zahlungsinstrument durchgeführt werden, mit dem Zahler vereinbart, sollte der Zahlungsdienstleister dem Zahler die Möglichkeit gewähren, diese Obergrenzen bis zum vereinbarten Höchstbetrag der Obergrenzen anzupassen.

96. Die Zahlungsdienstleister sollten den Zahlungsdienstnutzern die Möglichkeit gewähren, dass sie Warnungen bezüglich veranlasster oder fehlgeschlagener Versuche zur Auslösung von Zahlungsvorgängen erhalten, so dass sie eine betrügerische oder missbräuchliche Nutzung ihrer Konten erkennen können.

97. Die Zahlungsdienstleister sollten die Zahlungsdienstnutzer über Aktualisierungen der Sicherheitsverfahren informieren, die in Bezug auf die Erbringung von Zahlungsdiensten Auswirkungen auf die Zahlungsdienstnutzer haben.

98. Die Zahlungsdienstleister sollten die Zahlungsdienstnutzer in Bezug auf alle Fragen, Unterstützungsanfragen, Benachrichtigungen über Unregelmäßigkeiten oder alle sicherheitsrelevanten Fragen hinsichtlich der Zahlungsdienste unterstützen. Die Zahlungsdienstnutzer sollten angemessen darüber informiert werden, wie sie diese Unterstützung erhalten können.