EBA/GL/2017/05

11/09/2017

Leitlinien

Leitlinien für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (SREP)

1. 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 Artikel 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. Dazu sollten die zuständigen Behörden gemäß Artikel 2 Absatz 4 der Verordnung (EU) Nr. 1093/2010 die an sie gerichteten Leitlinien in geeigneter Weise in ihre Aufsichtspraktiken (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren) integrieren, einschließlich der Leitlinien in diesem Dokument, die in erster Linie an Institute gerichtet sind.

Meldepflichten

3. Nach Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden der EBA bis zum 13.11.2017 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/2017/05 “ an compliance@eba.europa.eu zu senden. Die Mitteilungen 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).

2. Gegenstand, Anwendungsbereich und Begriffsbestimmungen

Gegenstand und Anwendungsbereich

5. Diese Leitlinien, die gemäß Artikel 107 Absatz 3 der Richtlinie 2013/36/EU[2] ausgearbeitet wurden, zielen darauf ab, die Konvergenz der Aufsichtspraktiken bei der Bewertung des Informations- und Kommunikationstechnologie (IKT)-Risikos im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (SREP) sicherzustellen, auf den in Artikel 97 der Richtlinie 2013/36/EU Bezug genommen wird und der in den EBA-Leitlinien zu gemeinsamen Verfahren und Methoden für den aufsichtlichen Überprüfungs- und Bewertungsprozess (SREP)[3] näher spezifiziert wird. Insbesondere sind in diesen Leitlinien die Bewertungskriterien festgelegt, die die zuständigen Behörden bei der aufsichtlichen Bewertung der IKT-Governance und Strategie der Institute und bei der aufsichtlichen Bewertung der IKT-Risikopositionen und -kontrollen der Institute anwenden sollten. Diese Leitlinien bilden einen integralen Bestandteil der EBA-SREP-Leitlinien.

6. Die zuständigen Behörden sollten diese Leitlinien in Übereinstimmung mit dem in den EBA-SREP-Leitlinien festgelegten Anwendungsniveau des SREP und in Übereinstimmung mit dem darin festgelegten Mindestbeteiligungsmodell und den Verhältnismäßigkeitsanforderungen anwenden.

Adressaten

7. Diese Leitlinien richten sich an die zuständigen Behörden gemäß der Definition in Artikel 4 Absatz 2 Ziffer i der Verordnung (EU) Nr. 1093/2010.

Begriffsbestimmungen

8. Sofern nicht anders angegeben, haben die in der Richtlinie 2013/36/EU, in der Verordnung (EU) Nr. 575/2013 und in den Begriffsbestimmungen der EBA-SREP-Leitlinien verwendeten und definierten Begriffe in diesen Leitlinien dieselbe Bedeutung. Für die Zwecke dieser Leitlinien bezeichnet darüber hinaus der Begriff:

IKT-Systeme	eine IKT-Einrichtung als Teil eines Mechanismus oder eines einzelne Netze untereinander verbindenden Netzwerks, das die Betriebsaktivitäten eines Instituts unterstützt.

[2] Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (1), ABl. L 176 vom 27.6.2013.

[3] EBA/GL/2014/13

IKT-Dienstleistungen	Dienstleistungen, die von IKT-Systemen für einen oder mehrere interne oder externe Nutzer erbracht werden. Beispiele dafür sind Dienstleistungen in den Bereichen Datenerfassung, Datenspeicherung, Datenverarbeitung und Meldewesen, aber auch Überwachungs-, Geschäfts- und Entscheidungsunterstützungs-Dienstleistungen.
IKT-Verfügbarkeits- und Kontinuitätsrisiko	Das Risiko, dass die Leistung und die Verfügbarkeit von IKT-Systemen und -Daten nachteilig beeinflusst werden, einschließlich der mangelnden Fähigkeit infolge eines Ausfalls von IKT-Hardware- oder -Softwarekomponenten sie rechtzeitig wiederherzustellen; bzw. infolge von Schwächen im IKT-Systemmanagement oder eines sonstigen Ereignisses, die Dienste des Instituts, wie im Anhang weiter ausgeführt.
IKT-Sicherheitsrisiko	Das Risiko eines unbefugten Zugangs zu IKT-Systemen und Datenzugriffs von innerhalb oder außerhalb des Instituts (z. B. Cyber-Attacken), wie im Anhang weiter ausgeführt.
IKT-Änderungsrisiko	Das Risiko, das sich aus der mangelnden Fähigkeit des Instituts ergibt, IKT-Systemänderungen zeitgerecht und kontrolliert zu steuern, insbesondere was umfangreiche und komplexe Änderungsprogramme angeht, wie im Anhang weiter ausgeführt.
IKT-Datenintegritätsrisiko	Das Risiko, dass die von IKT-Systemen gespeicherten und verarbeiteten Daten über verschiedene IKT-Systeme hinweg unvollständig, ungenau oder inkonsistent sind, beispielsweise aufgrund mangelhafter oder fehlender IKT-Kontrollen während der verschiedenen Phasen des IKT-Datenlebenszyklus (d. h. Entwurf der Datenarchitektur, Entwicklung des Datenmodells und/oder der Datenbeschreibungsverzeichnisse, Überprüfung von Dateneingaben, Kontrolle von Datenextraktionen, -übertragungen und -verarbeitungen, einschließlich gerenderter Datenausgaben), was dazu führt, dass die Fähigkeit eines Instituts zur Erbringung von Dienstleistungen und zur ordnungsgemäßen und zeitgerechten Produktion von (Risiko-) Management- und Finanzinformationen beeinträchtigt wird, wie im Anhang weiter ausgeführt.
IKT-Auslagerungsrisiko	Das Risiko, dass die Beauftragung eines Dritten oder eines anderen Gruppenunternehmens (gruppeninterne Auslagerung) mit der Bereitstellung von IKT-Systemen oder der Erbringung damit zusammenhängender Dienstleistungen das Leistungs- und Risikomanagement des Instituts nachteilig beeinflusst, wie im Anhang weiter ausgeführt.

3. Umsetzung

Umsetzungsfrist

9. Diese Leitlinien gelten ab dem 1. Januar 2018.

4. Anforderungen an die IKT-Risikobewertung

Titel 1 - Allgemeine Bestimmungen

10. Die zuständigen Behörden sollten die Bewertung des IKT-Risikos sowie der Governance-Regeln und der IKT-Strategie im Rahmen des SREP-Prozesses gemäß dem in Titel 2 der EBA-SREP-Leitlinien festgelegten Mindestbeteiligungsmodell und gemäß den darin niedergelegten Verhältnismäßigkeitskriterien vornehmen. Dies bedeutet insbesondere Folgendes:

    a. die Häufigkeit der IKT-Risikobewertung würde von dem Mindestbeteiligungsmodell, das von der SREP-Kategorie angetrieben wird, der ein Institut zugeordnet ist, und seinem spezifischen aufsichtlichen Prüfprogramm abhängen, und

    b. die Gründlichkeit, Detailliertheit und Intensität der IKT-Bewertung sollten zur Größe, zur Struktur und zum betrieblichen Umfeld des Instituts sowie zur Art, zum Umfang und zur Komplexität seiner Tätigkeiten in einem angemessenen Verhältnis stehen.

11. Der Grundsatz der Verhältnismäßigkeit gilt in allen diesen Leitlinien für den Umfang, die Häufigkeit und die Intensität des aufsichtlichen Engagements und des Dialogs mit einem Institut sowie für die aufsichtlichen Erwartungen bezüglich der Standards, die das Institut erfüllen sollte.

12. Die zuständigen Behörden können sich auf die Arbeiten berufen, die bereits vom Institut oder von der zuständigen Behörde im Rahmen der Bewertung anderer Risiken oder SREP-Elemente durchgeführt wurden, und diese berücksichtigen, um eine Aktualisierung der Bewertung vorzunehmen. Bei der Durchführung der in diesen Leitlinien festgelegten Bewertungen sollten die zuständigen Behörden den Ansatz und die Methodik der aufsichtlichen Bewertung wählen, die am besten geeignet sind und die dem Institut angemessen sind, und die zuständigen Behörden sollten vorhandene und verfügbare Unterlagen (z. B. relevante Berichte und sonstige Unterlagen, Sitzungen mit (Risiko-) Management, Ergebnisse von Vor-Ort-Inspektionen) nutzen und diese in die Bewertung der zuständigen Behörden einfließen lassen.

13. Die zuständigen Behörden sollten die Ergebnisse ihrer Bewertungen der in diesen Leitlinien festgelegten Kriterien zusammenfassen und sie nutzen, um zu Schlussfolgerungen im Hinblick auf die Bewertung der SREP-Elemente gemäß den EBA-SREP-Leitlinien zu gelangen.

14. Insbesondere sollte die gemäß Titel 2 dieser Leitlinien durchgeführte Bewertung der Governance- und IKT-Strategie zu Ergebnissen führen, die in die Zusammenfassung der Ergebnisse der Bewertung der internen Governance und des institutsweiten Kontrollelements des SREP gemäß Titel 5 der EBA-SREP-Leitlinien einfließen und die jeweilige Punktebewertung dieses SREP-Elements widerspiegeln.

Ferner sollten die zuständigen Behörden berücksichtigen, dass wesentliche nachteilige Auswirkungen der IKT-Strategiebewertung auf die Geschäftsstrategie des Instituts oder etwaige Bedenken, dass das Institut möglicherweise nicht über ausreichende IKT-Ressourcen und IKT-Kapazitäten verfügt, um wichtige geplante strategische Änderungen durchzuführen und zu unterstützen, in die gemäß Titel 4 der EBA-SREP-Leitlinien durchgeführte Geschäftsmodellanalyse einfließen sollten.

15. Das Ergebnis der Bewertung des IKT-Risikos gemäß Titel 3 dieser Leitlinien sollte in die Ergebnisse der Bewertung des operationellen Risikos einfließen und als Einflussfaktor in Bezug auf die relevante Punktzahl gemäß Titel 6.4 der EBA-SREP-Leitlinien betrachtet werden.

16. Es wird darauf hingewiesen, dass, wenngleich die zuständigen Behörden die Unterkategorien von Risiken grundsätzlich als Teil der Hauptkategorien bewerten sollten (d. h. das IKT-Risiko wird als Bestandteil des operationellen Risikos bewertet), die zuständigen Behörden Unterkategorien auf individueller Basis bewerten können, wenn sie diese für erheblich erachten. Sollte das IKT-Risiko von der zuständigen Behörde als erhebliches Risiko ermittelt werden, so stellen diese Leitlinien zu diesem Zweck auch eine Bewertungstabelle zur Verfügung (Tabelle 1), die zur Bereitstellung einer eigenständigen Unterkategorie-Punktebewertung des IKT-Risikos gemäß dem Gesamtansatz zur Bewertung der Kapitalrisiken in den EBA-SREP-Leitlinien genutzt werden sollte.

17. Um zu prüfen, ob das IKT-Risiko als erheblich betrachtet werden sollte und daher die Möglichkeit besteht, dass das IKT-Risiko als einzelne Unterkategorie des operationellen Risikos zu beurteilen und mit Punkten zu bewerten ist, können die zuständigen Behörden die in Abschnitt 6.1 der EBA-SREP-Leitlinien festgelegten Kriterien verwenden.

18. Bei der Anwendung dieser Leitlinien sollten die zuständigen Behörden gegebenenfalls die nicht erschöpfende Liste der IKT-Risiko-Unterkategorien und Risikoszenarien, wie sie im Anhang aufgeführt sind, berücksichtigen, wobei im Anhang der Schwerpunkt auf IKT-Risiken liegt, die zu hohen Verlusten führen können. Die zuständigen Behörden können einige der in der Taxonomie enthaltenen IKT-Risiken ausschließen, falls diese für ihre Beurteilung nicht relevant sind. Es wird erwartet, dass die Institute ihre eigenen Risiko-Taxonomien beibehalten, statt die im Anhang aufgeführte IKT-Risiko-Taxonomie zu verwenden.

19. Werden Leitlinien in Verbindung mit grenzüberschreitenden Bankengruppen und deren Unternehmen angewandt und wurde ein Aufsichtskollegium eingerichtet, sollten die involvierten zuständigen Behörden im Rahmen ihrer Zusammenarbeit für die SREP-Bewertung gemäß Abschnitt 11.1 der EBA-SREP-Leitlinien den genauen und ausführlichen Anwendungsbereich jedes Informationselements konsequent für alle Gruppenunternehmen soweit wie möglich koordinieren.

Titel 2 - Bewertung der IKT-Governance und Strategie der Institute

2.1 Allgemeine Grundsätze

20. Die zuständigen Behörden sollten bewerten, ob der allgemeine Governance-Rahmen und der interne Kontrollrahmen des Instituts die IKT-Systeme und die damit verbundenen Risiken ordnungsgemäß abdecken und ob das Leitungsgremium diese Aspekte angemessen angeht und verwaltet, da die IKT für das ordnungsgemäße Funktionieren eines Instituts von integraler Bedeutung ist.

21. Bei der Durchführung dieser Bewertung sollten sich die zuständigen Behörden auf die Anforderungen und Standards für eine verantwortungsvolle interne Governance und die Risikokontrollregelungen beziehen, die in den EBA-Leitlinien für interne Governance (GL 44)[4] und in den internationalen Leitfaden in diesem Bereich festgelegt sind, soweit diese angesichts der Spezifität von IKT-Systemen und -Risiken anwendbar sind.

22. Die Bewertung in diesem Titel deckt nicht die spezifischen Elemente der IKT-System-Governance, des Risikomanagements und der Risikokontrollen ab, die auf die Steuerung spezifischer IKT-Risiken ausgerichtet sind, die unter Titel 3 dieser Leitlinien behandelt werden, sondern konzentriert sich auf folgende Bereiche:

    a. IKT-Strategie – ob das Institut über eine IKT-Strategie verfügt, die hinreichend geregelt ist und mit der Geschäftsstrategie des Instituts in Einklang steht;

    b. interne Governance – ob die internen Governance-Regelungen des Instituts in Bezug auf die IKT-Systeme des Instituts angemessen sind; und

    c. IKT-Risiko innerhalb des Risikomanagementrahmens – ob der Risikomanagementrahmen und der interne Kontrollrahmen des Instituts die IKT-Systeme des Instituts angemessen sichern.

23. Punkt a), auf den in Absatz 22 verwiesen wird, enthält Informationen über die Elemente der Governance des Instituts und sollte vor allem in die Bewertung des unter Titel 4 der EBA-SREP-Leitlinien dargelegten Geschäftsmodells einfließen. Die Punkte b) und c) stellen eine weitere Ergänzung zu den Bewertungen der Themen dar, die unter Titel 5 der EBA-SREP-Leitlinien niedergelegt sind, und die in diesen Leitlinien beschriebene Bewertung sollte in die jeweilige Bewertung gemäß Titel 5 der EBA-SREP-Leitlinien einfließen.

24. Das Ergebnis dieser Bewertung sollte gegebenenfalls in die Bewertung des Risikomanagements und der Risikokontrollen in Titel 3 dieser Leitlinien einfließen.

[4] EBA-Leitlinien für interne Governance, GL 44, 27. September 2011.

2.2 IKT-Strategie

25. Gemäß diesem Abschnitt sollten die zuständigen Behörden bewerten, ob das Institut über eine IKT-Strategie verfügt, die einer angemessenen Aufsicht durch das Leitungsorgan des Instituts unterliegt, welche im Einklang mit der Geschäftsstrategie steht, insbesondere im Hinblick auf die kontinuierliche Erneuerung der IKT und die Planung oder Umsetzung wichtiger und komplexer Änderungen im Bereich der IKT, und die das Geschäftsmodell des Instituts unterstützt.

2.2.1 Entwicklung und Angemessenheit der IKT-Strategie

26. Die zuständigen Behörden sollten bewerten, ob das Institut über einen Rahmen für die Ausarbeitung und Entwicklung der IKT-Strategie des Instituts verfügt, der im Einklang mit der Art, dem Umfang und der Komplexität seiner IKT-Tätigkeiten steht. Bei der Durchführung dieser Bewertung sollten die zuständigen Behörden berücksichtigen, ob:

    a. die Geschäftsleitung[5] des bzw. der Geschäftsbereiche angemessen an der Festlegung der strategischen IKT-Prioritäten des Instituts beteiligt ist, und die Geschäftsleitung der IKT-Funktion wiederum über die Entwicklung, Gestaltung und Initiierung wichtiger Geschäftsstrategien und -initiativen informiert ist, um die kontinuierliche Abstimmung zwischen IKT-Systemen, IKT-Diensten und der IKT-Funktion (d. h. die für die Verwaltung und den Einsatz dieser Systeme und Dienstleistungen verantwortlichen Personen) und der Geschäftsstrategie des Instituts sicherzustellen, und ob die IKT wirksam erneuert wird;

    b. die IKT-Strategie dokumentiert und durch konkrete Umsetzungspläne unterstützt wird, insbesondere in Bezug auf die wichtigen Meilensteine und die Ressourcenplanung (einschließlich der Finanz- und Humanressourcen), um sicherzustellen, dass sie realistisch sind und die Umsetzung der IKT-Strategie ermöglichen;

    c. das Institut seine IKT-Strategie insbesondere bei einer Änderung der Geschäftsstrategie regelmäßig überarbeitet, um eine kontinuierliche Abstimmung zwischen der IKT und den mittel- bis langfristigen Zielen, Plänen und Aktivitäten zu gewährleisten; und

    d. das Leitungsorgan des Instituts die IKT-Strategie und die Umsetzungspläne genehmigt und ihre Umsetzung überwacht.

2.2.2 Umsetzung der IKT-Strategie

27. Wenn die IKT-Strategie des Instituts die Umsetzung wichtiger und komplexer IKT-Änderungen oder Änderungen mit erheblichen Auswirkungen auf das Geschäftsmodell des Instituts erfordert, sollten die zuständigen Behörden bewerten, ob das Institut über einen Kontrollrahmen verfügt, der seiner Größe, seinen IKT-Aktivitäten und dem Grad der Änderungsaktivitäten angemessen ist, um die wirksame Umsetzung der IKT-Strategie des Instituts zu unterstützen. Bei der Durchführung dieser Bewertung sollten die zuständigen Behörden berücksichtigen, ob der Kontrollrahmen:

[5] Geschäftsleitung und Leitungsorgan gemäß den Definitionen in Richtlinie 2013/36/EU vom 26. Juni 2013 (Artikel 3 Ziffer 7: „Leitungsorgan“ und Artikel 3 Ziffer 9 „Geschäftsleitung“).

a. Governance-Prozesse (z. B. Fortschritts- und Haushaltsüberwachung und -berichterstattung) und relevante Stellen (z. B. ein Projektmanagementbüro, eine IKT-Lenkungsgruppe oder ähnliches) umfasst, um die Umsetzung der IKT-Strategieprogramme wirksam zu unterstützen;

b. die Rollen und Verantwortlichkeiten für die Umsetzung von IKT-Strategieprogrammen festgelegt und zugewiesen hat, wobei den Erfahrungen der wichtigsten Akteure bei der Organisation, Steuerung und Überwachung wichtiger und komplexer IKT-Änderungen und der Bewältigung der organisatorischen und menschlichen Auswirkungen (z. B. Umgang mit Widerstand gegen Änderungen, Schulung, Kommunikation) besondere Aufmerksamkeit geschenkt wird;

c. die unabhängige Kontrollfunktion und die Funktion „Innenrevision“ einbezieht, um sicherzustellen, dass die mit der Umsetzung der IKT-Strategie verbundenen Risiken ermittelt, bewertet und wirksam gemindert wurden, und dass der vorhandene Governance-Rahmen für die Umsetzung der IKT-Strategie wirksam ist; und

d. einen Planungs- und Planungsüberprüfungsprozess umfasst, der flexibel genug ist, um auf wichtige ermittelte Probleme (z. B. festgestellte Probleme oder Verzögerungen bei der Umsetzung) oder externe Entwicklungen (z. B. wichtige Veränderungen im Geschäftsumfeld, technologische Fragen oder Innovationen) zu reagieren, um eine rechtzeitige Anpassung der strategischen Umsetzung zu gewährleisten.

2.3 Allgemeine interne Governance

28. Gemäß Titel 5 der EBA-SREP-Leitlinien sollten die zuständigen Behörden bewerten, ob das Institut über eine angemessene und transparente Unternehmensstruktur verfügt, die „zweckdienlich“ ist und entsprechende Governance-Regeln umgesetzt hat. Unter besonderer Berücksichtigung der IKT-Systeme und im Einklang mit den EBA-Leitlinien für die interne Governance sollte im Rahmen dieser Bewertung geprüft werden, ob das Institut Folgendes nachweist:

    a. eine solide und transparente Organisationsstruktur mit klaren Zuständigkeiten in Bezug auf die IKT, einschließlich des Leitungsorgans und seiner Ausschüsse, und dass wichtige für IKT verantwortliche Personen (z. B. Chief Information Officer „CIO“, Chief Operating Officer „COO“ oder eine vergleichbare Rolle) über eine angemessene indirekte oder direkte Berichtslinie zu dem Leitungsorgan verfügen, um sicherzustellen, dass wichtige IKT-bezogene Informationen oder Probleme ordnungsgemäß gemeldet, erörtert und auf Ebene des Leitungsorgans entschieden werden; und

    b. dass das Leitungsorgan die mit der IKT verbundenen Risiken kennt und sie angeht.

29. Gemäß Abschnitt 5.2 der EBA-SREP-Leitlinien sollten die zuständigen Behörden bewerten, ob die IKT-Auslagerungspolitik und -strategie des Instituts gegebenenfalls die Auswirkungen der IKT-Auslagerung auf das Geschäft und das Geschäftsmodell des Instituts berücksichtigen.

2.4 IKT-Risiko im Risikomanagementrahmen des Instituts

30. Bei der Bewertung des institutsweiten Risikomanagements und der internen Kontrollen des Instituts gemäß Titel 5 der EBA-SREP-Leitlinien sollten die zuständigen Behörden prüfen, ob das Risikomanagement und das interne Kontrollsystem des Instituts die IKT-Systeme des Instituts angemessen und in einer Weise sichern, die der Größe und den Tätigkeiten des Instituts sowie seinem IKT-Risikoprofil gemäß Titel 3 entspricht. Die zuständigen Behörden sollten insbesondere Folgendes bestimmen:

    a. ob die Risikobereitschaft und die ICAAP die IKT-Risiken im Rahmen der breiteren operationellen Risikokategorie für die Bestimmung der Gesamtrisikostrategie und die Festlegung des Eigenkapitals abdecken; und

    b. ob die IKT-Risiken sich innerhalb des Anwendungsbereichs des institutsweiten Risikomanagementrahmens und des internen Kontrollrahmens befinden.

31. Die zuständigen Behörden sollten die Bewertung unter Punkt (a) oben unter Berücksichtigung sowohl erwarteter als auch nachteiliger Szenarien durchführen, z. B. Szenarien, die im institutsspezifischen oder aufsichtlichen Stresstest enthalten sind.

32. Unter besonderer Berücksichtigung von Punkt b) sollten die zuständigen Behörden bewerten, ob die in den Absätzen 104 (a), 104 (d), 105 (a) und 105 (c) der EBA-SREP-Leitlinien enthaltenen unabhängigen Kontroll- und internen Prüfungsfunktionen angemessen sind, um mit Blick auf die Größe und das IKT-Risikoprofil des Instituts eine ausreichende Unabhängigkeit zwischen der IKT und den Kontroll- und Prüfungsfunktionen zu gewährleisten.

2.5 Zusammenfassung der Feststellungen

33. Diese Ergebnisse sollten in der Zusammenfassung der Ergebnisse unter Titel 5 der EBA-SREP-Leitlinien wiedergegeben werden und in Übereinstimmung mit den Erwägungen in Tabelle 3 der EBA-SREP-Leitlinien in die jeweilige Punktebewertung einfließen.

34. Im Hinblick auf die Bewertung der IKT-Strategie sind bei der Fertigstellung der obigen Bewertung folgende Punkte zu berücksichtigen:

    a. Falls die zuständigen Behörden zu dem Schluss kommen, dass der Governance-Rahmen des Instituts für die Entwicklung und Umsetzung der IKT-Strategie des Instituts unter 2.2 nicht geeignet ist, sollte dies in die Bewertung der internen Governance des Instituts in Titel 5 der EBA-SREP-Leitlinien unter Absatz 87 (a) einfließen;

    b. falls die zuständigen Behörden aufgrund der oben genannten Bewertungen unter 2.2 zu dem Schluss kommen, dass es zu einer erheblichen fehlerhaften Angleichung zwischen der IKT-Strategie und der Geschäftsstrategie kommen würde, die erhebliche nachteilige Auswirkungen auf die langfristigen Geschäfts- und/oder Finanzziele des Instituts, die Nachhaltigkeit des Instituts und/oder sein Geschäftsmodell oder die Geschäftsfelder bzw. -bereiche des Instituts hätte, welche in Absatz 62 (a) der EBA-SREP-Leitlinien als äußerst

erheblich eingestuft wurden, so sollte dies in die Geschäftsmodellbewertung von Titel 4 der EBA-SREP-Leitlinien unter Absatz 70 (b) und (c) einfließen; und

c. falls die zuständigen Behörden aufgrund der oben genannten Bewertungen unter Punkt 2.2 zu dem Schluss kommen, dass die IKT-Ressourcen und IKT-Umsetzungskapazitäten des Instituts womöglich nicht ausreichen, um wichtige geplante Änderungen an der Strategie durchzuführen und zu unterstützen, sollte dies in die Geschäftsmodellbewertung von Titel 4 der EBA-SREP-Leitlinien unter Absatz 70 (b) einfließen.

Titel 3 - Bewertung der IKT-Risikopositionen und -kontrollen der Institute

3.1 Allgemeine Überlegungen

35. Die zuständigen Behörden sollten bewerten, ob das Institut seine IKT-Risiken ordnungsgemäß ermittelt, bewertet und gemindert hat. Dieser Prozess sollte Teil des operationellen Risikomanagementrahmens sein und mit dem auf das operationelle Risiko anwendbaren Ansatz kongruent sein.

36. Die zuständigen Behörden sollten zunächst die erheblichen inhärenten IKT-Risiken ermitteln, denen das Institut ausgesetzt ist oder sein könnte; daran sollte sich eine Bewertung der Wirksamkeit des IKT-Risikomanagementrahmens und der Verfahren und Kontrollen zur Minderung dieser Risiken anschließen. Das Ergebnis der Bewertung sollte sich in einer Zusammenfassung der Feststellungen widerspiegeln, die in die Punktzahl des operationellen Risikos in den EBA-SREP-Leitlinien einfließt. Wenn das IKT-Risiko als erheblich eingestuft wird und die zuständigen Behörden eine einzelne Punktzahl vergeben möchten, sollte Tabelle 1 verwendet werden, um eine Punktzahl als Teilrisiko des operationellen Risikos zu vergeben.

37. Bei der Durchführung der Bewertung unter diesem Titel sollten die zuständigen Behörden alle verfügbaren Informationsquellen als Grundlage für die Ermittlung ihrer aufsichtlichen Bewertungsprioritäten verwenden, wie in Absatz 127 von Titel 6 der EBA-SREP-Leitlinien angegeben, z. B. die Risikomanagementaktivitäten, die Berichterstattung und die Ergebnisse des Instituts. Die zuständigen Behörden sollten auch andere Informationsquellen nutzen, um diese Bewertung durchzuführen, einschließlich gegebenenfalls:

    a. Selbstbewertungen von IKT-Risiko und Kontrollen (falls in den ICAAP-Informationen enthalten);
    b. mit dem IKT-Risiko verbundene Managementinformationen (MI), die dem Leitungsorgan des Instituts vorgelegt werden, z. B. periodische und ereignisbezogene IKT-Risikoberichterstattung (auch in der Datenbank zu den Betriebsverlusten), IKT-Risiko-Positionsdaten aus der Risikomanagementfunktion des Instituts;
    c. IKT-bezogene interne und externe Prüfungsfeststellungen, die dem Prüfungsausschuss des Instituts übermittelt werden.

3.2 Ermittlung erheblicher IKT-Risiken

38. Die zuständigen Behörden sollten unter Berücksichtigung der nachstehenden Schritte die erheblichen IKT-Risiken ermitteln, denen das Institut ausgesetzt ist oder ausgesetzt sein könnte.

3.2.1 Überprüfung des IKT-Risikoprofils des Instituts

39. Bei der Überprüfung des IKT-Risikoprofils des Instituts sollten die zuständigen Behörden alle relevanten Informationen über die IKT-Risikopositionen des Instituts, einschließlich der Informationen gemäß

Absatz 37 und der festgestellten erheblichen Mängel oder Schwachstellen in der IKT-Organisation und den institutsweiten Kontrollen unter Titel 2 dieser Leitlinien, berücksichtigen und diese Informationen gegebenenfalls in einer angemessenen Weise überprüfen. Im Rahmen dieser Überprüfung sollten die zuständigen Behörden Folgendes berücksichtigen:

a. die potenziellen Auswirkungen einer erheblichen Störung der IKT-Systeme des Instituts auf das Finanzsystem auf nationaler oder internationaler Ebene;
b. ob das Institut aufgrund von Internet-Abhängigkeiten, einer hohen Akzeptanz innovativer IKT-Lösungen oder anderen geschäftlichen Vertriebskanälen, die es zu einem wahrscheinlichen Ziel für Cyber-Angriffe machen, womöglich IKT-Sicherheitsrisiken und IKT-Verfügbarkeits- und Kontinuitätsrisiken ausgesetzt ist;
c. ob das Institut aufgrund seiner komplexen (z. B. infolge von Fusionen oder Akquisitionen) oder veralteten IKT-Systeme womöglich in verstärktem Maße IKT-Sicherheitsrisiken, IKT-Verfügbarkeits- und Kontinuitätsrisiken, IKT-Datenintegritätsrisiken oder IKT-Änderungsrisiken ausgesetzt ist;
d. ob das Institut erhebliche Änderungen an seinen IKT-Systemen und/oder seiner IKT-Funktion vornimmt (z. B. durch Fusionen, Akquisitionen, Desinvestitionen oder den Austausch ihrer IKT-Kernsysteme), die die Stabilität oder das ordnungsgemäße Funktionieren der IKT-Systeme beeinträchtigen können und zu erheblichen IKT-Verfügbarkeits- und Kontinuitätsrisiken, IKT-Sicherheitsrisiken, IKT-Änderungsrisiken oder IKT-Datenintegritätsrisiken führen können;
e. ob das Institut IKT-Dienstleistungen oder IKT-Systeme innerhalb oder außerhalb der Gruppe ausgelagert hat, wodurch es erheblichen IKT-Auslagerungsrisiken ausgesetzt sein kann;
f. ob das Institut aggressive IKT-Kostensenkungsmaßnahmen durchführt, die eine Reduzierung der erforderlichen IKT-Investitionen, Ressourcen und IT-Kompetenzen bewirken können und die Exposition gegenüber allen IKT-Risikoarten in der Taxonomie erhöhen können;
g. ob der Standort wichtiger IKT-Maßnahmen/Rechenzentren (z. B. Regionen, Länder) das Institut Naturkatastrophen (z. B. Überschwemmungen, Erdbeben), politischer Instabilität oder Arbeitskonflikten und zivilen Unruhen aussetzen kann, die zu einer erheblichen Zunahme der IKT-Verfügbarkeits- und Kontinuitätsrisiken und der IKT-Sicherheitsrisiken führen können.

3.2.2 Überprüfung der kritischen IKT-Systeme und -Dienste

40. Im Rahmen des Prozesses zur Ermittlung der IKT-Risiken mit potenziell erheblichen aufsichtlichen Auswirkungen auf das Institut sollten die zuständigen Behörden die Unterlagen des Instituts überprüfen und eine Stellungnahme dazu abgeben, welche IKT-Systeme und -Dienste für eine ordnungsgemäße Funktionsweise, Verfügbarkeit, Kontinuität und Sicherheit der wesentlichen Tätigkeiten des Instituts von entscheidender Bedeutung sind.

41. Zu diesem Zweck sollten die zuständigen Behörden die vom Institut angewandten Methoden und Prozesse überprüfen, um die kritischen IKT-Systeme und -Dienste zu ermitteln, wobei zu berücksichtigen ist, dass einige IKT-Systeme und -Dienste vom Institut im Hinblick auf die Geschäftskontinuität und die Verfügbarkeit, im Hinblick auf die Sicherheit (z. B. Betrugsverhütung) und/oder im Hinblick auf die Vertraulichkeit (z. B. vertrauliche Daten) als kritisch betrachtet werden können. Bei der Durchführung

der Überprüfung sollten die zuständigen Behörden berücksichtigen, dass kritische IKT-Systeme und -Dienste mindestens eine der folgenden Bedingungen erfüllen sollten:

a. sie unterstützen das Kerngeschäft und die Vertriebskanäle (z. B. Geldautomaten, Online- und Mobile Banking) des Instituts;

b. sie unterstützen wesentliche Governance-Prozesse und Unternehmensfunktionen, einschließlich des Risikomanagements (z. B. Risikomanagementsysteme sowie Systeme zur Verwaltung der Finanzmittel);

c. sie unterliegen besonderen gesetzlichen oder aufsichtlichen Anforderungen (falls vorhanden), die für einige systemrelevante Dienste (falls und wo zutreffend) erhöhte Verfügbarkeits-, Ausfallsicherheits-, Vertraulichkeits- oder Sicherheitsanforderungen erforderlich machen (z. B. Datenschutzgesetze oder mögliche „Recovery Time Objectives“ (RTO, d. h. die maximale Zeitspanne, innerhalb derer ein System oder ein Prozess nach einem Ereignis wiederhergestellt werden muss) und „Recovery Point Objective“ (RPO, d. h. die maximale Zeitspanne, innerhalb derer Daten im Falle eines Ereignisses verloren gehen können);

d. sie verarbeiten oder speichern vertrauliche oder sensible Daten, bei denen sich ein unberechtigter Zugriff in erheblichem Maße auf den Ruf des Instituts, das Finanzergebnis oder die Solidität und Kontinuität seines Geschäfts (z. B. Datenbanken mit sensiblen Kundendaten) auswirken könnte; und/oder

e. sie bieten Basisfunktionen, die für das angemessene Funktionieren des Instituts (z. B. Telekommunikations- und Konnektivitätsdienste, IKT- und Cybersicherheitsdienste) von entscheidender Bedeutung sind.

3.2.3 Ermittlung erheblicher IKT-Risiken für kritische IKT-Systeme und -Dienste

42. Unter Berücksichtigung der durchgeführten Überprüfungen des IKT-Risikoprofils und der oben genannten kritischen IKT-Systeme und -Dienste des Instituts sollten die zuständigen Behörden eine Stellungnahme zu den erheblichen IKT-Risiken abgeben, die ihrem aufsichtlichen Urteil zufolge erhebliche aufsichtliche Auswirkungen auf die kritischen IKT-Systeme und -Dienste des Instituts haben können.

43. Bei der Bewertung der potenziellen Auswirkungen von IKT-Risiken auf die kritischen IKT-Systeme und -Dienste eines Instituts sollten die zuständigen Behörden Folgendes berücksichtigen:

a. die finanziellen Auswirkungen, einschließlich (aber nicht beschränkt auf) den Verlust von Geldmitteln oder Vermögenswerten, potenzielle Kundenentschädigungen, Gerichts- und Sanierungskosten, vertraglichen Schadenersatz, Einnahmeausfälle;

b. das Potenzial für Betriebsstörungen, unter Berücksichtigung (aber nicht beschränkt auf) die Kritikalität der betroffenen Finanzdienstleistungen, die Anzahl der potenziell betroffenen Kunden und/oder Zweigstellen und Mitarbeiter;

c. die potenziellen Auswirkungen auf die Reputation des Instituts auf der Grundlage der Kritikalität der betroffenen Bankdienstleistung oder Geschäftstätigkeit (z. B. Diebstahl von Kundendaten), das

externe Profil bzw. die externe Sichtbarkeit der betroffenen IKT-Systeme und -Dienste (z. B. Mobile- oder Online-Banking-Systeme, Verkaufsstellen, Geldautomaten oder Zahlungssysteme);

d. die regulatorischen Auswirkungen, einschließlich potenzieller öffentlicher Kritik durch die Aufsichtsbehörde, Geldstrafen oder sogar eine Änderung von Zulassungen;

e. die strategischen Auswirkungen auf das Institut, z. B. wenn strategische Produktpläne oder Geschäftspläne gefährdet oder gestohlen werden.

44. Die zuständigen Behörden sollten sodann die ermittelten IKT-Risiken, die als erheblich eingestuft werden, in die folgenden IKT-Risikokategorien eintragen, für die im Anhang zusätzliche Risikobeschreibungen und Beispiele bereitgestellt wurden. Die zuständigen Behörden sollten über die IKT-Risiken im Anhang im Rahmen der Bewertung unter Titel 3 nachdenken:

a. IKT-Verfügbarkeits- und Kontinuitätsrisiko
b. IKT-Sicherheitsrisiko
c. IKT-Änderungsrisiko
d. IKT-Datenintegritätsrisiko
e. IKT-Auslagerungsrisiko

Die Einteilung in Kategorien dient dazu, den zuständigen Behörden dabei zu helfen, zu bestimmen, welche Risiken erheblich sind (falls zutreffend) und deshalb in den folgenden Bewertungsschritten einer näheren und/oder eingehenderen Überprüfung unterzogen werden sollten.

3.3 Bewertung der Kontrollen zur Minderung erheblicher IKT-Risiken

45. Um die verbleibende IKT-Risikoposition des Instituts zu bewerten, sollten die zuständigen Behörden prüfen, wie das Institut die von den zuständigen Behörden in der obigen Bewertung ermittelten erheblichen Risiken ermittelt, überwacht, einstuft und mindert.

46. Zu diesem Zweck sollten die zuständigen Behörden im Hinblick auf die ermittelten erheblichen IKT-Risiken das Zutreffende überprüfen:

a. IKT-Risikomanagementrichtlinien, -prozesse und Risikotoleranzschwellen;

b. Organisationsmanagement- und Aufsichtsrahmen;

c. interner Prüfungsumfang und -feststellungen; und

d. IKT-Risikokontrollen, die für das ermittelte erhebliche IKT-Risiko spezifisch sind.

47. Bei der Bewertung sollten das Ergebnis der Analyse des Gesamtrisikomanagement- und internen Kontrollrahmens, wie in Titel 5 der EBA-SREP-Leitlinien erwähnt, sowie die Governance und Strategie des Instituts gemäß Titel 2 dieser Leitlinien berücksichtigt werden, da signifikante Mängel, die in diesen Bereichen identifiziert wurden, die Fähigkeit des Instituts zur Steuerung und Minderung seiner IKT-Risikopositionen beeinträchtigen können. Soweit erforderlich, sollten die zuständigen Behörden auch die Informationsquellen in Absatz 37 dieser Leitlinien nutzen.

48. Die zuständigen Behörden sollten die folgenden Bewertungsschritte in einer Weise durchführen, die der Art, dem Umfang und der Komplexität der Tätigkeiten des Instituts angemessen ist, und dabei eine aufsichtlichen Überprüfung vornehmen, die dem IKT-Risikoprofil des Instituts angemessen ist.

3.3.1 IKT-Risikomanagementpolitik, -prozesse und -toleranzschwellen

49. Die zuständigen Behörden sollten prüfen, ob das Institut über geeignete Risikomanagementpolitiken, -prozesse und -toleranzschwellen für die ermittelten erheblichen IKT-Risiken verfügt. Diese können Teil des operationellen Risikomanagementrahmens oder eines separaten Dokuments sein. Bei dieser Bewertung sollten die zuständigen Behörden berücksichtigen, ob:

    a. die Risikomanagementrichtlinien vom Leitungsorgan formalisiert und genehmigt wurde und hinreichende Richtlinien in Bezug auf die IKT-Risikobereitschaft des Instituts und die wichtigsten IKT-Risikomanagementziele und/oder angewandten IKT-Risikotoleranzschwellen enthält. Außerdem sollten alle relevanten Stakeholder über die relevante IKT- Risikomanagementrichtlinien informiert werden;

    b. die anwendbare Politik alle wesentlichen Elemente für das Risikomanagement der ermittelten erheblichen IKT-Risiken umfasst;

    c. das Institut einen Prozess und zugrunde liegende Verfahren zur Ermittlung (z. B. „Risikokontroll-Selbstbewertung“, Risikoszenarioanalyse) und Überwachung der einbezogenen erheblichen IKT-Risiken umgesetzt hat; und

    d. das Institut über eine Berichtslinie zum IKT-Risikomanagement verfügt, die der Geschäftsleitung und dem Leitungsorgan zeitgerechte Informationen zur Verfügung stellt und der Geschäftsleitung und/oder dem Leitungsorgan die Möglichkeit gibt, zu bewerten und zu kontrollieren, ob die IKT-Risikominderungspläne und -maßnahmen des Instituts mit den genehmigten Risikobereitschafts- und/oder -toleranzschwellen (soweit relevant) übereinstimmen, und Änderungen erheblicher IKT-Risiken zu überwachen.

3.3.2 Organisationsmanagement- und Aufsichtsrahmen

50. Die zuständigen Behörden sollten bewerten, wie die anwendbaren Risikomanagement-Rollen und -Verantwortlichkeiten in die interne Organisation eingebettet und integriert werden, um die ermittelten erheblichen IKT-Risiken zu steuern und zu überwachen. In diesem Zusammenhang sollten die zuständigen Behörden bewerten, ob das Institut Folgendes nachweist:

    a. klare Rollen und Verantwortlichkeiten für die Ermittlung, Bewertung, Überwachung, Minderung, Meldung und Überwachung des damit verbundenen erheblichen IKT-Risikos;

    b. dass die Risikoverantwortlichkeiten und -rollen in allen relevanten Teilen (z. B. Geschäftsbereiche, IT) und Prozessen der Organisation klar kommuniziert, zugewiesen und eingebettet werden, einschließlich der Rollen und Verantwortlichkeiten für die Erhebung und Aggregation der Risikodaten und ihrer Berichterstattung an die Geschäftsleitung und/oder das Leitungsorgan;

    c. dass die IKT-Risikomanagement-Aktivitäten mit ausreichenden und qualitativ angemessenen personellen und technischen Mitteln durchgeführt werden. Zur Bewertung

der Glaubwürdigkeit der anwendbaren Risikominderungspläne sollten die zuständigen Behörden auch beurteilen, ob das Institut ausreichende Finanzmittel und/oder sonstige für ihre Umsetzung erforderlichen Mittel bereitgestellt hat;

d. eine angemessene Nachbereitung und Reaktion des Leitungsorgans auf wichtige Feststellungen der unabhängigen Kontrollfunktionen hinsichtlich des oder der IKT-Risiken unter Berücksichtigung der möglichen Delegierung einiger Aspekte an einen Ausschuss, soweit vorhanden; und
e. dass Ausnahmen von den anwendbaren IKT-Vorschriften und -Regeln erfasst und einer dokumentierten Überprüfung und Berichterstattung durch die unabhängige Kontrollfunktion unter Berücksichtigung der damit verbundenen Risiken unterzogen werden.

3.3.3 Interner Prüfungsumfang und -feststellungen

51. Die zuständigen Behörden sollten beurteilen, ob die Innenrevision im Hinblick auf die Prüfung des anwendbaren IKT-Risikokontrollrahmens wirksam ist, indem sie überprüft, ob:

a. der IKT-Risikokontrollrahmen mit der geforderten Qualität, Gründlichkeit und Häufigkeit geprüft und er der Größe, den Aktivitäten und dem IKT-Risikoprofil des Instituts entspricht;
b. der Prüfungsplan die Prüfung der vom Institut ermittelten kritischen IKT-Risiken berücksichtigt;
c. die wichtigen IKT-Prüfungsfeststellungen, einschließlich der vereinbarten Maßnahmen, dem Leitungsorgan mitgeteilt werden; und
d. IKT-Prüfungsfeststellungen, einschließlich vereinbarter Maßnahmen, nachverfolgt und Fortschrittsberichte von der Geschäftsleitung und/oder dem Prüfungsausschuss regelmäßig überprüft werden.

3.3.4 IKT-Risikokontrollen, die für die ermittelten erheblichen IKT-Risiken spezifisch sind

52. Für die ermittelten erheblichen IKT-Risiken sollten die zuständigen Behörden bewerten, ob das Institut spezifische Kontrollen zur Bewältigung dieser Risiken eingeführt hat. Die folgenden Abschnitte enthalten eine nicht erschöpfende Liste der spezifischen Kontrollen, die bei der Bewertung der unter Punkt 3.2.3 genannten erheblichen Risiken zu berücksichtigen sind, welche den folgenden IKT-Risikokategorien zugeordnet wurden:

a. IKT-Verfügbarkeits- und Kontinuitätsrisiken,
b. IKT-Sicherheitsrisiken,
c. IKT-Änderungsrisiken,
d. IKT-Datenintegritätsrisiken,
e. IKT-Auslagerungsrisiken.

(a) Kontrollen für den Umgang mit erheblichen IKT-Verfügbarkeits- und Kontinuitätsrisiken

53. Neben den Anforderungen der EBA-SREP-Leitlinien (Absätze 279-281) sollten die zuständigen Behörden bewerten, ob das Institut über einen geeigneten Rahmen zur Ermittlung, zum Verständnis, zur Messung und zur Minderung der IKT-Verfügbarkeits- und Kontinuitätsrisiken verfügt.

54. Bei dieser Bewertung sollten die zuständigen Behörden insbesondere berücksichtigen, ob der Rahmen:

a. die kritischen IKT-Prozesse und die entsprechenden unterstützenden IKT-Systeme, die Teil der Notfall- und Kontinuitätspläne sein sollten, ermittelt, und zwar mit:

   i. einer umfassenden Analyse der Abhängigkeiten zwischen den kritischen Geschäftsprozessen und Unterstützungssystemen;

   ii. der Bestimmung der Wiederherstellungsziele für die unterstützenden IKT-Systeme (z. B. in der Regel vom Geschäftsbereich und/oder den Vorschriften in Bezug auf RTO und RPO bestimmt);

   iii. angemessener Notfallplanung, um die Verfügbarkeit, Kontinuität und Wiederherstellung kritischer IKT-Systeme und -Dienste zu ermöglichen mit dem Ziel, Störungen der Tätigkeiten eines Instituts in vertretbaren Grenzen zu halten.

b. über Richtlinien und Standards in Bezug auf Notfallpläne, die Kontinuitätskontrollumgebung und operationelle Kontrollen verfügt, die Folgendes beinhalten:

   i. Maßnahmen, um zu vermeiden, dass ein einzelnes Szenario, Ereignis oder Katastrophe Auswirkungen auf sowohl die IKT-Produktions- als auch die IKT-Wiederherstellungssysteme haben könnte,

   ii. IKT-System-Backup- und Wiederherstellungsverfahren für kritische Software und Daten, die sicherstellen, dass diese Backups an einem sicheren und ausreichend entfernt gelegenen Ort gespeichert werden, so dass ein Ereignis oder eine Katastrophe diese kritischen Daten nicht zerstören oder beschädigen können;

   iii. Überwachungslösungen zur zeitgerechten Aufdeckung von IKT-Verfügbarkeits- oder Kontinuitätsereignissen;

   iv. einen dokumentierten Ereignismanagement- und -eskalationsprozess, der Orientierungshilfen für die verschiedenen Ereignismanagement- und eskalationsrollen und -verantwortlichkeiten, die Mitglieder des bzw. der Krisenausschüsse und die Befehlskette in Notfällen vorgibt;

   v. physische Maßnahmen, um die kritische IKT-Infrastruktur des Instituts (z. B. Rechenzentren) vor Umweltrisiken (z. B. Überschwemmungen und anderen Naturkatastrophen) zu schützen und eine angemessene Betriebsumgebung für IKT-Systeme (z. B. Klimaanlage) sicherzustellen;

   vi. Prozesse, Rollen und Verantwortlichkeiten, um sicherzustellen, dass auch ausgelagerte IKT-Systeme und -Dienste von angemessenen Notfall- und Kontinuitätslösungen und -plänen abgedeckt werden;

   vii. IKT-Leistungs- und Kapazitätsplanungs- sowie Überwachungslösungen für kritische IKT-Systeme und -Dienste mit festgelegten Verfügbarkeitsanforderungen, um rechtzeitig wichtige Leistungs- und Kapazitätseinschränkungen zu ermitteln;

   viii. Lösungen zum Schutz kritischer Internetaktivitäten oder -dienste (z. B. E-Banking-Dienste), soweit erforderlich und angemessen, gegen Denial-of-Service- und anderen Cyber-Angriffen

aus dem Internet, die darauf abzielen, den Zugriff zu diesen Aktivitäten und Diensten zu verhindern oder zu stören.

c. die IKT-Verfügbarkeits- und Kontinuitätslösungen mit Blick auf eine Reihe realistischer Szenarien prüft, darunter Cyber-Angriffe, Failover-Tests und Backup-Tests für kritische Software und Daten, die:

   i. geplant, formalisiert und dokumentiert sind, und die Testergebnisse, die zur Stärkung der Wirksamkeit der IKT-Verfügbarkeits- und Kontinuitätslösungen genutzt werden;

   ii. Stakeholder und Funktionen innerhalb der Organisation beinhalten, wie Geschäftsbereichsmanagement einschließlich der Geschäftskontinuitäts-, Ereignis- und Krisenreaktionsteams, sowie relevante externe Stakeholder im Ökosystem;

   iii. das Leitungsorgan und die Geschäftsleitung entsprechend beteiligt (als Teil der Krisenmanagementteams) und über die Testergebnisse informiert sind.

(b) Kontrollen für den Umgang mit erheblichen IKT-Sicherheitsrisiken

55. Die zuständigen Behörden sollten bewerten, ob das Institut über einen wirksamen Rahmen zur Ermittlung, Verständnis, Messung und Minderung des IKT-Sicherheitsrisikos verfügt. Bei dieser Bewertung sollten die zuständigen Behörden insbesondere prüfen, ob der Rahmen Folgendes berücksichtigt:

a. klar definierte Rollen und Verantwortlichkeiten in Bezug auf:
   i. die Person(en) und/oder Ausschüsse, die für das tägliche IKT-Sicherheitsmanagement und die Ausarbeitung der übergreifenden IKT-Sicherheitspolitiken verantwortlich oder diesbezüglich rechenschaftspflichtig sind, unter Beachtung ihrer erforderlichen Unabhängigkeit;
   ii. die Gestaltung, Umsetzung, Verwaltung und Überwachung von IKT-Sicherheitskontrollen;
   iii. der Schutz kritischer IKT-Systeme und -Dienste, z. B. durch Verabschiedung eines Sicherheitslücken-Bewertungsprozesses, Software-Patch-Management, durchgehenden Schutz (z. B. Schadsoftware-Virus), Eindringungserkennungs- und Präventionstools;
   iv. die Überwachung, Klassifizierung und Behandlung externer oder interner IKT-Sicherheitsereignisse, einschließlich der Ereignisreaktion und der Wiederinbetriebnahme und Wiederherstellung der IKT-Systeme und -Dienste;
   v. regelmäßige und proaktive Bedrohungsbewertungen zur Aufrechterhaltung angemessener Sicherheitskontrollen.

b. eine IKT-Sicherheitspolitik, die international anerkannte IKT-Sicherheitsstandards und Sicherheitsgrundsätze (z. B. das „Prinzip der geringsten Privilegien", d. h. die Begrenzung des Zugriffs auf das absolute Minimum, um ein normales Funktionieren der Verwaltung der Zugriffsrechte zu erlauben, und das Prinzip der „Verteidigung in der Tiefe“, d. h. überlagerte Sicherheitsmechanismen, welche die Sicherheit des Systems als Ganzes zur Entwicklung einer Sicherheitsarchitektur erhöhen) berücksichtigt und gegebenenfalls einhält;

c. ein Prozess zur Ermittlung von IKT-Systemen, -Diensten und angemessenen Sicherheitsanforderungen, die ein potenzielles Betrugsrisiko und/oder eine unsachgemäße oder missbräuchliche Verwendung vertraulicher Daten widerspiegeln, sowie einzuhaltende dokumentierte Sicherheitserwartungen für diese ermittelten IKT-Systeme, -Dienste und -Daten, die auf die Risikotoleranz des Instituts abgestimmt sind, und deren ordnungsgemäße Umsetzung überwacht wird;

d. einen dokumentierten Sicherheitsereignismanagement- und -eskalationsprozess, der Orientierungshilfen für die verschiedenen Ereignismanagement- und -eskalationsrollen und -verantwortlichkeiten, die Mitglieder des bzw. der Krisenausschüsse und die Befehlskette in Notfällen bei Sicherheitsproblemen vorgibt;

e. Protokollierung der Nutzer- und Administratorenaktivität, um eine wirksame Überwachung und die rechtzeitige Aufdeckung und Reaktion auf unbefugte Zugriffe zu ermöglichen; um forensische Untersuchungen von Sicherheitsereignissen zu unterstützen oder durchzuführen. Das Institut sollte über Protokollierungsleitfaden verfügen, in der angemessene Protokolltypen sowie ihre Aufbewahrungszeiträume festgelegt sind;

f. Sensibilisierungs- und Informationskampagnen oder -initiativen, um alle Ebenen des Instituts über die sichere Nutzung und den Schutz der IKT-Systeme des Instituts und die wichtigsten IKT-Sicherheitsrisiken (und andere) Risiken zu informieren, über die sie Bescheid wissen sollten, insbesondere hinsichtlich der bestehenden und sich entwickelnden Cyberrisiken (z. B. Computerviren, mögliche interne oder externe Missbräuche oder Angriffe, Cyber-Angriffe) und ihre Rolle bei der Minderung von Sicherheitsverstößen;

g. angemessene physische Sicherheitsmaßnahmen (z. B. Videoüberwachung, Einbruchalarm, Sicherheitstüren), um einen unbefugten physischen Zugriff auf kritische und sensible IKT-Systeme (z. B. Rechenzentren) zu verhindern;

h. Maßnahmen zum Schutz der IKT-Systeme vor Angriffen aus dem Internet (d. h. Cyber-Angriffe) oder anderen externen Netzwerken (z. B. traditionelle Telekommunikationsverbindungen oder Verbindungen mit vertrauenswürdigen Partnern). Die zuständigen Behörden sollten prüfen, ob der Rahmen des Instituts Folgendes berücksichtigt:

    i. einen Prozess und Lösungen zum Führen eines vollständigen und aktuellen Inventars und einer Übersicht über alle nach außen gerichteten Netzwerkverbindungspunkte (z. B. Websites, Online-Anwendungen, WLAN, Fernzugriff), durch die Dritte in die internen IKT-Systeme eindringen könnten.

    ii. genau gesteuerte und überwachte Sicherheitsmaßnahmen (z. B. Firewalls, Proxy-Server, Mail-Relays, Antivirus- und Content-Scanner), um den eingehenden und ausgehenden Netzwerkverkehr (z. B. E-Mail) und die nach außen gerichteten Netzwerkverbindungen, durch die Dritte in die internen IKT-Systeme eindringen könnten, zu sichern;

    iii. Prozesse und Lösungen zur Sicherung von Websites und Anwendungen, die direkt aus dem Internet und/oder von außen angegriffen werden können und als Zugriffspunkt in die internen IKT-Systeme dienen können. In der Regel handelt es sich dabei um eine Kombination aus anerkannten sicheren Entwicklungspraktiken, IKT-Systemhärtungs- und Sicherheitslücken-Scanning-Praktiken und/oder die Implementierung ergänzender

Sicherheitslösungen, wie z. B. Anwendungs-Firewalls und/oder Eindringungserkennungs- und/oder Präventionstools;

iv. regelmäßige Sicherheitsdurchdringungstests zur Bewertung der Wirksamkeit von implementierten Cyber- und internen IKT-Sicherheitsmaßnahmen und -prozessen. Diese Tests sollten von Mitarbeitern und/oder externen Sachverständigen mit dem erforderlichen Fachwissen durchgeführt werden, wobei dokumentierte Testergebnisse und Schlussfolgerungen der Geschäftsleitung und/oder dem Leitungsorgan mitgeteilt werden. Soweit erforderlich und anwendbar, sollte das Institut aus diesen Tests Erkenntnisse im Hinblick darauf ziehen, an welchen Stellen die Sicherheitskontrollen und -prozesse weiter verbessert werden können und/oder wie eine bessere Sicherung ihrer Wirksamkeit bewerkstelligt werden kann.

(c) Kontrollen für den Umgang mit erheblichen IKT-Änderungsrisiken

56. Die zuständigen Behörden sollten bewerten, ob das Institut über einen wirksamen Rahmen für die Ermittlung, das Verständnis, die Messung und die Minderung des IKT-Änderungsrisikos verfügt, das der Art, dem Umfang und der Komplexität der Tätigkeiten des Instituts und dem IKT-Risikoprofil des Instituts angemessen ist. Der Rahmen des Instituts sollte die Risiken umfassen, die mit der Entwicklung, dem Testen und der Genehmigung von Änderungen der IKT-Systeme verbunden sind, einschließlich der Entwicklung oder Änderung von Software, bevor sie in die Produktionsumgebung migriert werden, und ein angemessenes IKT-Lebenszyklusmanagement gewährleisten. Bei dieser Bewertung sollten die zuständigen Behörden insbesondere prüfen, ob der Rahmen Folgendes berücksichtigt:

a. dokumentierte Prozesse zur Verwaltung und Kontrolle von Änderungen an IKT-Systemen (z. B. Konfigurations- und Patch-Management) und Daten (z. B. Fehlerbehebung oder Datenkorrekturen), um eine angemessene Einbindung des IKT-Risikomanagements für wichtige IKT-Änderungen zu gewährleisten, die das Risikoprofil oder die Risikoposition des Instituts erheblich beeinträchtigen können;

b. Spezifikationen im Hinblick auf die erforderliche Aufgabentrennung in den verschiedenen Phasen der implementierten IKT-Änderungsprozesse (z. B. Lösungskonzept und -entwicklung, Prüfung und Genehmigung neuer Software und/oder Änderungen, Migration und Implementierung in der Produktionsumgebung und Fehlerbehebung) mit Schwerpunkt auf den implementierten Lösungen und der Aufgabentrennung in Verwaltung und Kontrolle von Änderungen an den IKT-Produktionssystemen und -daten durch IKT-Mitarbeiter (z. B. Entwickler, IKT-Systemadministratoren, Datenbankadministratoren) oder eine andere Partei (z. B. geschäftliche Nutzer, Dienstanbieter);

c. Testumgebungen, die die Produktionsumgebungen angemessen widerspiegeln;

d. ein Asset-Inventar der bestehenden Anwendungen und IKT-Systeme in der Produktionsumgebung sowie die Test- und Entwicklungsumgebung, so dass erforderliche Änderungen (z. B. Versions-Updates oder -Upgrades, System-Patching, Konfigurationsänderungen) für die beteiligten IKT-Systeme ordnungsgemäß verwaltet, implementiert und überwacht werden können.

e. ein Prozess für Lebenszyklusmanagement und -überwachung der verwendeten IKT-Systeme, um sicherzustellen, dass sie weiterhin die tatsächlichen Anforderungen an das Geschäfts- und

Risikomanagement erfüllen und unterstützen und dafür sorgen, dass die verwendeten IKT-Lösungen und -Systeme weiterhin von ihren Anbietern unterstützt werden; und dass dies mit angemessenen Prozessen zum Softwareentwicklungs-Lebenszyklus einhergeht.

f. ein Software-Quellcode-Kontrollsystem und entsprechende Verfahren zur Verhütung unbefugter Änderungen im Quellcode der intern entwickelten Software;

g. ein Prozess zur Durchführung eines Sicherheits- und Sicherheitslücken-Screenings von neuen oder erheblich modifizierten IKT-Systemen und Software, bevor sie zur Produktion freigegeben und möglichen Cyber-Angriffen ausgesetzt werden;

h. ein Prozess und Lösungen zur Verhinderung der unbefugten oder unbeabsichtigten Freigabe vertraulicher Daten beim Austausch, Archivieren, Entsorgen oder Vernichten von IKT-Systemen;

i. ein unabhängiger Überprüfungs- und Validierungsprozess zur Reduzierung der Risiken in Bezug auf menschliche Fehler bei der Durchführung von Änderungen an den IKT-Systemen, die erhebliche nachteilige Auswirkungen auf die Verfügbarkeit, Kontinuität oder Sicherheit des Instituts (z. B. wichtige Änderungen an der Firewall-Konfiguration) oder auf die Sicherheit des Instituts (z. B. Änderungen an den Firewalls) haben können.

(d) Kontrollen für den Umgang mit erheblichen IKT-Datenintegritätsrisiken

57. Die zuständigen Behörden sollten bewerten, ob das Institut über einen wirksamen Rahmen für die Ermittlung, das Verständnis, die Messung und die Minderung des IKT-Datenintegritätsrisikos verfügt, das der Art, dem Umfang und der Komplexität der Tätigkeiten des Instituts und dem IKT-Risikoprofil des Instituts angemessen ist. Im Rahmen des Instituts sollten die Risiken berücksichtigt sein, die mit der Wahrung der Integrität der von den IKT-Systemen gespeicherten und verarbeiteten Daten verknüpft sind. Bei dieser Bewertung sollten die zuständigen Behörden insbesondere prüfen, ob in dem Rahmen Folgendes berücksichtigt ist:

a. Richtlinien, in denen die Rollen und Verantwortlichkeiten für die Verwaltung der Integrität der Daten in den IKT-Systemen festgelegt sind (z. B. Datenarchitekten, Datensachbearbeiter[6], Datentreuhänder[7], Dateneigentümer/-verwalter[8]) und in der Orientierungshilfen dazu enthalten sind, welche Daten im Hinblick auf die Datenintegrität kritisch sind und spezifischen IKT-Kontrollen (z. B. automatisierte Eingabevalidierungskontrollen, Datenübertragungskontrollen, Datenabgleichen usw.) oder Überprüfungen (z. B. eine Kompatibilitätsprüfung mit der Datenarchitektur) in den verschiedenen Phasen des IKT-Datenlebenszyklus unterzogen werden sollten;

b. eine dokumentierte Datenarchitektur, ein Datenmodell und/oder ein Datenbeschreibungsverzeichnis, das mit relevanten Geschäfts- und IT-Stakeholdern validiert wird, um die erforderliche Datenkohärenz in den IKT-Systemen zu unterstützen und

[6] Ein Datensachbearbeiter ist für die Datenverarbeitung und -nutzung zuständig.
[7] Ein Datentreuhänder ist für sichere Aufbewahrung, den Transport und die Speicherung von Daten zuständig.
[8] Ein Datenverwalter ist für die Verwaltung und die Tauglichkeit von Datenelementen – sowohl der Inhalte und der Metadaten – zuständig.

sicherzustellen, dass die Datenarchitektur, das Datenmodell und/oder das Datenbeschreibungsverzeichnis auf die Geschäfts- und Risikomanagement-Erfordernisse abgestimmt sind;

c. eine Richtlinien im Hinblick auf die zulässige Nutzung und Vertrauenswürdigkeit von End User Computing, insbesondere hinsichtlich der Ermittlung, Registrierung und Dokumentation wichtiger Endbenutzer-Computing-Lösungen (z. B. bei der Verarbeitung wichtiger Daten) und der erwarteten Sicherheitsstufe zur Verhütung unbefugter Änderungen sowohl im Tool selbst als auch in den darin gespeicherten Daten;

d. dokumentierte Ausnahmebehandlungsprozesse, um ermittelte IKT-Datenintegritätsprobleme gemäß ihrer Kritikalität und Empfindlichkeit zu lösen.

58. Für beaufsichtigte Institute, die in den Anwendungsbereich der BCBS 239-Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung[9] fallen, sollten die zuständigen Behörden die Risikoanalyse des Instituts in Bezug auf seine Risikoberichterstattung und seine Datenaggregationskapazitäten im Vergleich zu den Grundsätzen und den auf ihrer Grundlage erstellten Unterlagen überprüfen und dabei den Umsetzungszeitplan und Übergangsregelungen in diesen Grundsätzen berücksichtigen.

(e) Kontrollen für den Umgang mit erheblichen IKT-Auslagerungsrisiken

59. Die zuständigen Behörden sollten bewerten, ob die Auslagerungsstrategie des Instituts, die mit den Anforderungen der CEBS-Auslagerungsleitlinien (2006) und ferner mit der Anforderung in Absatz 85 (d) der EBA-SREP-Leitlinien in Einklang steht, ordnungsgemäß auf die IKT-Auslagerung, einschließlich der gruppeninternen Auslagerung zur Erbringung von IKT-Dienstleistungen innerhalb der Gruppe, Anwendung findet. Bei der Bewertung der IKT-Auslagerungsrisiken sollten die zuständigen Behörden berücksichtigen, dass die IKT-Auslagerungsrisiken auch im Rahmen der Bewertung der inhärenten operationellen Risiken nach Absatz 240 (j) der EBA-SREP-Leitlinien abgedeckt werden können, um jegliche Doppelarbeit oder Doppelzählung zu vermeiden.

60. Insbesondere sollten die zuständigen Behörden bewerten, ob das Institut über einen wirksamen Rahmen für die Ermittlung, das Verständnis und die Bewertung des IKT-Auslagerungsrisikos und insbesondere über Kontrollen und ein Kontrollumfeld zur Minderung von Risiken in Bezug auf erhebliche IKT-Auslagerungsdienste verfügt, die der Größe, den Aktivitäten und dem IKT-Risikoprofil des Instituts angemessen sind und Folgendes enthalten:

a. eine Bewertung der Auswirkungen der IKT-Auslagerung auf das Risikomanagement des Instituts im Zusammenhang mit der Nutzung von Dienstanbietern (z. B. Cloud-Dienstanbietern) und deren Dienstleistungen während des Beschaffungsprozesses, die dokumentiert und von der Geschäftsleitung oder dem Leitungsorgan bei der Entscheidung für oder gegen die Auslagerung der Dienste berücksichtigt wird. Das Institut sollte die IKT-Risikomanagementpolitiken sowie die IKT-Kontrollen und das Kontrollumfeld des Dienstanbieters überprüfen, um sicherzustellen, dass sie die

[9] Basler Ausschuss für Bankenaufsicht, Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung, Januar 2013, online verfügbar: http://www.bis.org/publ/bcbs239_de.pdf.

internen Ziele im Hinblick auf das Risikomanagement und die Risikobereitschaft erfüllen. Diese Überprüfung sollte während des vertraglichen Auslagerungszeitraums regelmäßig aktualisiert werden, wobei die Merkmale der ausgelagerten Dienstleistungen zu berücksichtigen sind;

b. eine Überwachung der IKT-Risiken der ausgelagerten Dienstleistungen während des vertraglichen Auslagerungszeitraums im Rahmen des Risikomanagements des Instituts, die in die IKT-Risikomanagement-Berichterstattung des Instituts einfließt (z. B. Geschäftskontinuitäts-Berichterstattung, Sicherheitsberichterstattung);

c. eine Überwachung und ein Vergleich der erhaltenen Dienstleistungsniveaus mit den vertraglich vereinbarten Dienstleistungsniveaus, die Bestandteil des Auslagerungsvertrags oder der Dienstleistungsvereinbarung (SLA) sein sollten; und

d. geeignete Mitarbeiter, Ressourcen und Kompetenzen zur Überwachung und Steuerung der IKT-Risiken, die von den ausgelagerten Dienstleistungen ausgehen.

3.4 Zusammenfassung der Feststellungen und der Punktebewertung

61. Im Anschluss an die oben genannte Bewertung sollten die zuständigen Behörden eine Stellungnahme zum IKT-Risiko des Instituts abgeben. Diese Stellungnahme sollte in einer Zusammenfassung der Feststellungen zum Ausdruck kommen, die die zuständigen Behörden bei der Vergabe der Punktebewertung des operationellen Risikos in Tabelle 6 der EBA-SREP-Leitlinien berücksichtigen sollten. Die zuständigen Behörden sollten ihre Sicht auf erhebliche IKT-Risiken auf die folgenden Überlegungen stützen, die in die operationelle Risikobewertung einfließen sollten:

a. Risikoüberlegungen

   i. Das IKT-Risikoprofil und -positionen des Instituts;
   ii. die ermittelten kritischen IKT-Systeme und -Dienstleistungen; und
   iii. Die Erheblichkeit des IKT-Risikos bei kritischen IKT-Systemen.

b. Überlegungen hinsichtlich Management und Kontrollen

   i. Ob die IKT-Risikomanagementpolitik und -strategie des Instituts und seine Gesamtstrategie und Risikobereitschaft kohärent sind;
   ii. ob der organisatorische Rahmen für das IKT-Risikomanagement robust ist und klare Verantwortlichkeiten und eine klare Aufgabentrennung zwischen Risikoeignern und Management- und Kontrollfunktionen bestehen;
   iii. ob die IKT-Risikomessungs-, -überwachungs- und -meldesysteme angemessen sind; und
   iv. ob die Kontrollrahmen für erhebliche IKT-Risiken intakt sind.

62. Wenn die zuständigen Behörden davon ausgehen, dass das IKT-Risiko erheblich ist, und die zuständige Behörde beschließt, dieses Risiko als Unterkategorie des operationellen Risikos zu prüfen und mit Punkten zu bewerten, enthält die nachstehende Tabelle (Tabelle 1) die Überlegungen zur IKT-Risiko-Punktebewertung.

Tabelle 1: Aufsichtliche Überlegungen zur Vergabe einer IKT-Risiko-Punktzahl

Risiko-Punktzahl	Aufsichtlicher Standpunkt	Überlegungen zum inhärenten Risiko	Überlegungen zur angemessenen Steuerung und Kontrolle
1	Es besteht kein erkennbares Risiko erheblicher aufsichtlicher Auswirkungen auf das Institut angesichts der Höhe des inhärenten Risikos und der Steuerung und Kontrollen.	• Die gemäß Absatz 37 zu berücksichtigenden Informationsquellen zeigten keine signifikanten IKT-Risikopositionen. • Die Art des IKT-Risikoprofils des Instituts in Verbindung mit der Überprüfung der kritischen IKT-Systeme und der erheblichen IKT-Risiken für die IKT-Systeme und -Dienstleistungen haben keine erheblichen IKT-Risiken ergeben.	• Die IKT-Risikopolitik und -strategie des Instituts ist der Gesamtstrategie und der Risikobereitschaft angemessen. • Der organisatorische Rahmen für das IKT-Risiko ist robust, und es bestehen klare Verantwortlichkeiten und eine klare Aufgabentrennung zwischen Risikoeignern und Management- und Kontrollfunktionen. • Die IKT-Risikomessungs-, -überwachungs- und -meldesysteme sind angemessen. • Der Kontrollrahmen für das IKT-Risiko ist intakt.
2	Es besteht ein geringes Risiko erheblicher aufsichtlicher Auswirkungen auf das Institut angesichts der Höhe des inhärenten Risikos und der Steuerung und Kontrollen.	• Die gemäß Absatz 37 zu berücksichtigenden Informationsquellen zeigten keine signifikanten IKT-Risikopositionen. • Die Art des IKT-Risikoprofils des Instituts in Verbindung mit der Überprüfung der kritischen IKT-Systeme und der erheblichen IKT-Risiken für die IKT-Systeme und -Dienstleistungen haben eine begrenzte IKT-Risikoposition ergeben (z. B. nicht mehr als zwei von fünf der vordefinierten IKT-Risikokategorien).	
3	Es besteht ein mittleres Risiko erheblicher aufsichtlicher Auswirkungen auf das Institut unter Berücksichtigung des inhärenten Risikos und der Steuerung und Kontrollen.	• Die gemäß Absatz 37 zu berücksichtigenden Informationsquellen zeigten Hinweise auf mögliche signifikante IKT-Risikopositionen. • Die Art des IKT-Risikoprofils des Instituts in Verbindung mit der Überprüfung der kritischen IKT-Systeme und der erheblichen IKT-Risiken für die IKT-Systeme und -Dienstleistungen haben eine erhöhte IKT-Risikoposition ergeben (z. B. drei oder mehr von fünf der vordefinierten	

		IKT-Risikokategorien).	
4	Es besteht ein hohes Risiko erheblicher aufsichtlicher Auswirkungen auf das Institut angesichts der Höhe des inhärenten Risikos und der Steuerung und Kontrollen.	• Die gemäß Absatz 37 zu berücksichtigenden Informationsquellen zeigten mehrere Hinweise auf signifikante IKT-Risikopositionen. • Die Art des IKT-Risikoprofils des Instituts in Verbindung mit der Überprüfung der kritischen IKT-Systeme und der erheblichen IKT-Risiken für die IKT-Systeme und -Dienstleistungen haben eine hohe IKT-Risikoposition ergeben (z. B. vier oder fünf von fünf der vordefinierten IKT-Risikokategorien).	

Anhang - IKT-Risikotaxonomie

Fünf IKT-Risikokategorien mit einer nicht erschöpfenden Liste von potenziell schwerwiegenden IKT-Risiken und/oder IKT-Risiken mit operationellen, reputationsbezogenen oder finanziellen Auswirkungen

IKT-Risiko-kategorien	IKT-Risiken (nicht erschöpfend[10])	Risikobeschreibung	Beispiele
IKT-Verfügbarkeits- und Kontinuitäts-risiken	Unangemessenes Kapazitäts-management	Ein Mangel an Ressourcen (z. B. Hardware, Software, Personal, Dienstanbieter) kann dazu führen, dass die Dienstleistung die Geschäftsanforderungen nicht erfüllt, und kann außerdem zu Systemunterbrechungen, einer Verschlechterung von Dienstleistungs- und/oder Betriebsfehlern führen.	• Ein Mangel an Kapazitäten kann sich auf die Übertragungsraten und die Verfügbarkeit des Netzwerks (Internet) für Dienste wie Online-Banking auswirken. • Ein Personalmangel (internes Personal oder Personal eines Dritten) kann zu Systemunterbrechungen und/oder Betriebsfehlern führen.
	IKT-Systemausfälle	Eine Beeinträchtigung der Verfügbarkeit aufgrund von Hardwareausfällen.	• Ausfall/Fehlfunktion der Speicherung (Festplatten), Server oder anderer IKT-Geräte, z. B. verursacht durch mangelnde Wartung.
		Eine Beeinträchtigung der Verfügbarkeit aufgrund von Softwarefehlern und Bugs.	• Endlosschleife in Anwendungssoftware verhindert die Ausführung der Transaktion. • Ausfälle durch den fortgesetzten Einsatz veralteter IKT-Systeme und -Lösungen, die nicht mehr den aktuellen Verfügbarkeits- und Resilienzanforderungen entsprechen und/oder nicht mehr von ihren Anbietern unterstützt werden.
	Unangemessene IKT-Kontinuitäts- und Notfall-Wiederher-stellungsplanung	Ausfall von geplanten IKT-Verfügbarkeits- und/oder Kontinuitätslösungen und/oder Notfall-Wiederherstellung (z. B. Fall-Back-Wiederherstellungs-Rechenzentrum) bei Aktivierung in Reaktion auf ein Ereignis.	• Konfigurationsunterschiede zwischen dem primären und dem sekundären Rechenzentrum können dazu führen, dass das Fall-Back-Rechenzentrum nicht in der Lage ist, die geplante Kontinuität des Dienstes bereitzustellen.

[10] Die IKT-Risiken sind unter der Risikokategorie aufgeführt, auf die sie die meisten Auswirkungen haben, aber sie können sich auch auf andere Risikokategorien auswirken.

IKT-Risiko-kategorien	IKT-Risiken (nicht erschöpfend[10])	Risikobeschreibung	Beispiele
	Disruptive und zerstörerische Cyber-Angriffe	Angriffe zu unterschiedlichen Zwecken (z. B. Aktivismus, Erpressung), die zu einer Überlastung von Systemen und des Netzwerks führen, wodurch verhindert wird, dass legitime Nutzer auf ihre Online-Computerdienste zugreifen können.	• Distributed Denial-of-Service-Angriffe werden von einer Vielzahl an Computersystemen im Internet durchgeführt, die von einem Hacker gesteuert werden; dabei wird eine große Menge an scheinbar legitimen Dienstanfragen an Online-Dienste gestellt (z. B. Online-Banking).
IKT-Sicherheits-risiken	Cyber-Angriffe und sonstige externe IKT-basierte Angriffe	Angriffe, die aus dem Internet oder aus externen Netzwerken zu unterschiedlichen Zwecken durchgeführt werden (z. B. Betrug, Spionage, Aktivismus/Sabotage, Cyber-Terrorismus), wobei eine Vielzahl von Techniken eingesetzt wird (z. B. Social Engineering, Eindringversuche durch Ausnutzung von Sicherheitslücken, Einsatz von Schadprogrammen) und die Kontrolle über interne IKT-Systeme übernommen wird.	Verschiedene Arten von Angriffen: • APT (Advanced Persistent Threat) zwecks Übernahme der Kontrolle über interne Systeme oder Datendiebstahl (z. B. Daten im Zusammenhang mit Identitätsdiebstahl, Kreditkarteninformationen). • Schadsoftware (z. B. Ransomware), die Daten zu Zwecken der Erpressung verschlüsselt. • Infizierung interner IKT-Systeme mit Trojanern zwecks verdeckter Durchführung systemschädigender Aktionen. • Ausnutzung von Sicherheitslücken des IKT-Systems und/oder einer (Web-)Anwendung (z. B. SQL-Einschleusung), um Zugang zum internen IKT-System zu erhalten.
		Ausführung betrügerischer Zahlungsvorgänge durch Hacker durch die Unterbrechung oder Umgehung der Sicherheitsvorkehrungen von E-Banking- und Zahlungsdiensten und/oder durch den Angriff auf und die Ausnutzung von Sicherheitslücken in den internen Zahlungssystemen des Instituts.	• Angriffe gegen E-Banking- oder Zahlungsdienste mit dem Ziel der Ausführung nicht autorisierter Transaktionen. • Die Erstellung und der Versand betrügerischer Zahlungsanweisungen von innerhalb des internen Zahlungssystems des Instituts (z. B. betrügerische SWIFT-Mitteilungen).
		Ausführung betrügerischer Wertpapiertransaktionen durch Hacker durch die Unterbrechung oder Umgehung der Sicherheitsvorkehrungen der E-Banking-Dienste, die auch den Zugriff auf die Wertpapierdepots des	• Pump-and-Dump-Angriffe, bei denen die Angreifer Zugriff auf die E-Banking-Wertpapierdepots von Kunden erhalten und betrügerische Kauf- oder Verkaufsaufträge veranlassen, um den Marktpreis zu beeinflussen und/oder Gewinne auf der Basis

IKT-Risiko-kategorien	IKT-Risiken (nicht erschöpfend[10])	Risikobeschreibung	Beispiele
		Kunden ermöglichen.	von früheren Wertpapierpositionen zu erzielen.
		Angriffe auf Kommunikationsverbindungen und Gespräche aller Art oder IKT-Systeme mit dem Ziel, Informationen zu sammeln und/oder Betrug zu begehen.	• Abhören/Abfangen der ungeschützten Übertragung von Authentifizierungsdaten im Klartext.
	Unangemessene interne IKT-Sicherheit	Ermöglichung eines uneingeschränkten Zugriffs auf kritische IKT-Systeme innerhalb des Instituts zu unterschiedlichen Zwecken (z. B. Betrug, Durchführung und Verschleierung unlauterer Geschäftspraktiken, Datendiebstahl, Aktivismus/Sabotage) unter Einsatz einer Vielzahl von Techniken (z. B. Missbrauch und/oder Eskalation von Privilegien, Identitätsdiebstahl, Social Engineering, Ausnutzung von Sicherheitslücken in IKT-Systemen, Einsatz von Schadsoftware).	• Installation von Tastenanschlags-Loggern (Key-Logger), um Benutzer-IDs und Passwörter zu stehlen und dadurch einen unbefugten Zugriff auf vertrauliche Daten zu erhalten und/oder Betrug zu begehen. • Knacken/Erraten schwacher Passwörter, um illegitime oder erweiterte Zugriffsrechte zu erhalten. • Systemadministrator nutzt Betriebssysteme oder Datenbankeinrichtungen (für direkte Datenbankänderungen), um Betrug zu begehen.
		Unbefugte IKT-Manipulationen infolge von unangemessenen IKT-Zugriffsmanagementverfahren und -praktiken.	• Es wurde versäumt, nicht benötigte Konten zu deaktivieren oder zu löschen, wie z. B. Konten von Mitarbeitern, die in eine andere Funktion gewechselt sind und/oder das Institut verlassen haben, einschließlich Besuchern oder Lieferanten, die keinen Zugriff mehr benötigen, wodurch ein unberechtigter Zugriff auf IKT-Systeme ermöglicht wurde. • Vergabe übermäßiger Zugriffsrechte und Privilegien zur Ermöglichung unbefugter Zugriffe und/oder Verschleierung unlauterer Praktiken.
		Sicherheitsbedrohungen aufgrund mangelnden Sicherheitsbewusstseins, wobei die Mitarbeiter die IKT-Sicherheitspolitiken und -verfahren nicht verstehen, sie vernachlässigen oder nicht einhalten.	• Mitarbeiter, die getäuscht werden, um unwissentllich einen Angriff zu unterstützen (d. h. Social Engineering). • Mangelhafte Praktiken in Bezug auf Anmeldeinformationen: Weitergabe von

IKT-Risiko-kategorien	IKT-Risiken (nicht erschöpfend[10])	Risikobeschreibung	Beispiele
			Passwörtern, „leicht“ zu erratende Passwörter, Verwendung desselben Passworts für viele verschiedene Zwecke usw. • Speicherung unverschlüsselter vertraulicher Daten auf Laptops und tragbaren Datenspeicherlösungen (z. B. USB-Sticks), die verloren gehen oder gestohlen werden können.
		Die unbefugte Speicherung oder Übertragung vertraulicher Daten außerhalb des Instituts.	• Personen, die vertrauliche Informationen stehlen oder absichtlich veröffentlichen oder herausschmuggeln und gegenüber unbefugten Personen oder der Öffentlichkeit offenlegen.
	Unangemessene physische IKT-Sicherheit	Missbrauch oder Diebstahl von IKT-Vermögenswerten über einen physischen Zugang mit Schäden, Verlust von Vermögenswerten, Datenverlust oder Ermöglichung weiterer Bedrohungen als Folge.	• Einbruch in Bürogebäude und/oder Rechenzentren, um IKT-Geräte (z. B. Computer, Laptops, Speicherlösungen) zu stehlen und/oder durch physischen Zugriff auf IKT-Systeme Daten zu kopieren.
		Absichtliche oder versehentliche Schäden an physischen IKT-Vermögenswerten durch Terrorismus, Unfälle oder unglückliche/fehlerhafte Manipulationen durch Mitarbeiter des Instituts und/oder Dritte (Lieferanten, Reparateure).	• Physischer Terrorismus (d. h. Bombenanschläge) oder Sabotage von IKT-Vermögenswerten. • Zerstörung von Rechenzentren durch Brände, Wasserlecks oder andere Faktoren.
		Ungenügender physischer Schutz vor Naturkatastrophen, der zur teilweisen oder vollständigen Zerstörung der IKT-Systeme/Rechenzentren durch Naturkatastrophen führt.	• Erdbeben, extreme Hitze, Stürme, starke Schneestürme, Überschwemmung, Brände, Blitzschlag.

IKT-Änderungs-risiken	Unangemessene Kontrollen von IKT-Systemände-rungen und IKT-Entwicklungen	Ereignisse, die durch unentdeckte Fehler oder Sicherheitslücken aufgrund von Änderungen, z. B. an Software, IKT-Systemen und Daten, verursacht werden (z. B. unvorhergesehene Auswirkungen einer Änderung oder einer schlecht gesteuerten Änderung aufgrund mangelnder Tests oder nicht ordnungsgemäßer Änderungsmanagementpraktiken).	• Produktionsfreigabe von unzureichend getesteter Software oder Konfigurationsänderungen mit unerwarteten nachteiligen Auswirkungen auf Daten (z. B. Beschädigung, Löschung) und/oder die IKT-Systemleistung (z. B. Systemausfall, Leistungsverschlechterung). • Unkontrollierte Änderungen an den IKT-Systemen oder Daten in der Produktionsumgebung. • Produktionsfreigabe unzureichend gesicherter IKT-Systeme und Internetanwendungen, wodurch Möglichkeiten für Hacker geschaffen werden, die bereitgestellten Online-Dienste anzugreifen und/oder die internen IKT-Systeme zu beschädigen. • Unkontrollierte Änderungen am Quellcode intern entwickelter Software. • Unzureichende Tests aufgrund eines Mangels an angemessenen Testumgebungen.
	Unangemessene IKT-Architektur	Ein mangelhaftes IKT-Architekturmanagement bei der Entwicklung, dem Aufbau und der Wartung von IKT-Systemen (z. B. Software, Hardware, Daten) kann im Laufe der Zeit zu komplexen, schwierigen, kostspieligen und starren IKT-Systemen führen, die nicht mehr ausreichend auf die Geschäftsanforderungen abgestimmt sind und die tatsächlichen Anforderungen in Bezug auf das Risikomanagement nicht erfüllen.	• Unzureichend gesteuerte Änderungen an IKT-Systemen, Software und/oder Daten über einen längeren Zeitraum, die zu komplexen, heterogenen und schwer zu steuernden IKT-Systemen und -Architekturen führen und viele nachteilige Auswirkungen auf das Geschäft und das Risikomanagement haben (z. B. fehlende Flexibilität und Agilität, IKT-Ereignisse und -Ausfälle, hohe Betriebskosten, geschwächte IKT-Sicherheit und -Resilienz, reduzierte Datenqualität und Berichterstattungskapazitäten). • Übermäßige Anpassung an kundenspezifische Anforderungen und Erweiterungen kommerzieller Softwarepakete mit intern entwickelter Software, was dazu führt, dass zukünftige Releases und Upgrades der kommerziellen Software nicht implementiert werden können und das Risiko

			besteht, dass diese nicht länger vom Hersteller unterstützt werden.
	Unangemessenes Lebenszyklus- und Patch-Management	Das Fehlen eines angemessenen Inventars aller IKT-Vermögenswerte zur Unterstützung von und in Kombination mit funktionierenden Lebenszyklus- und Patch-Management-Praktiken. Dies führt zu unzureichend gepatchten (und damit anfälligeren) und veralteten IKT-Systemen, die die Anforderungen des Geschäfts und des Risikomanagements womöglich nicht unterstützen.	• Ungepatchte und veraltete IKT-Systeme, die nachteilige Auswirkungen auf das Geschäft und das Risikomanagement haben können (z. B. fehlende Flexibilität und Agilität, IKT-Ausfälle, geschwächte IKT-Sicherheit und -Resilienz).
IKT-Datenintegritäts-risiken	Dysfunktionale IKT-Datenverarbei-tung oder Handhabung	Aufgrund von System-, Kommunikations- und/oder Anwendungsfehlern oder -ausfällen oder fehlerhaft ausgeführten Datenextraktions-, Übertragungs- und Lade- (ETL-) Prozessen können Daten beschädigt werden oder verloren gehen.	• IT-Systemfehler in der Batchverarbeitung, was zu falschen Salden auf den Bankkonten des Kunden führt. • Falsch ausgeführte Anfragen. • Datenverlust durch Datenreplikations- (Backup-) Fehler.
	Fehlerhaft konstruierte Datenvalidie-rungskontrollen in IKT-Systemen	Fehler im Zusammenhang mit fehlenden oder ineffektiven automatisierten Dateneingabe- und Datenannahme-Kontrollen (z. B. für gebrauchte Daten von Drittanbietern), Datenübertragungs-, Datenverarbeitungs- und Datenausgabekontrollen in den IKT-Systemen (z. B. Eingabevalidierungskontrollen, Datenabstimmungen).	• Unzureichende oder ungültige Formatierung/Validierung von Dateneingaben in Anwendungen und/oder Benutzeroberflächen. • Fehlende Datenabstimmungskontrollen von produzierten Ausgaben • Fehlende Kontrollen in Bezug auf die ausgeführten Datenextraktionsprozesse (z. B. Datenbankabfragen), was zu fehlerhaften Daten führt. • Verwendung fehlerhafter externer Daten.
	Fehlerhaft kontrollierte Datenänderungen in den IKT-Produktions-systemen.	Datenfehler, die aufgrund fehlender Kontrollen in Bezug auf die Korrektheit und Zulässigkeit von Datenmanipulationen bei der Produktion von IKT-Systemen entstanden sind.	• Entwickler oder Datenbankadministratoren, die direkt auf die Daten der IKT-Systeme in einer nicht kontrollierten Weise zugreifen und diese ändern, z. B. im Falle eines IKT-Ereignisses.
	Fehlerhaft konstruierte	Fehlerhaft gesteuerte Datenarchitekturen, Datenmodelle, Datenströme oder	• Das Bestehen unterschiedlicher Kundendatenbanken je Produkt- oder

	und/oder gesteuerte Datenarchitektur, Datenströme, Datenmodelle oder Datenbeschrei-bungsver-zeichnisse	Datenbeschreibungsverzeichnisse können dazu führen, dass es mehrere Versionen derselben Daten in den IKT-Systemen gibt, die aufgrund von unterschiedlich angewandten Datenmodellen oder Datendefinitionen und/oder Unterschieden im zugrundeliegenden Datengenerierungs- und Datenänderungsprozess nicht mehr konsistent sind.	Geschäftseinheit mit unterschiedlichen Datendefinitionen und -feldern führt zu unabgestimmten und schwer zu vergleichenden integrierten Kundendaten auf der Ebene des gesamten Finanzinstituts oder der gesamten Finanzgruppe.
IKT-Auslagerungs-risiken	Unzureichende Resilienz der Dienste von Drittanbietern oder anderer Gruppen-unternehmen	Die Nichtverfügbarkeit kritischer IKT-Auslagerungsdienste, Telekommunikationsdienste und -einrichtungen. Verlust oder Beschädigung kritischer/sensibler Daten, die dem Dienstanbieter anvertraut sind	• Nichtverfügbarkeit wesentlicher Dienste durch Ausfälle in (ausgelagerten) IKT-Systemen oder Anwendungen von Lieferanten. • Unterbrechung von Telekommunikationsverbindungen. • Stromversorgungslücken.
	Unangemessene Auslagerungs-politik	Wesentliche Verschlechterung der Dienste oder Ausfälle aufgrund ineffizienter Vorbereitung oder Kontrollprozesse des ausgelagerten Dienstanbieters. Eine ineffiziente Auslagerungspolitik kann zu einem Mangel an geeigneten Kompetenzen und Kapazitäten im Hinblick auf die vollständige Ermittlung, Bewertung, Minderung und Überwachung der IKT-Risiken führen und die operativen Kapazitäten der Institute einschränken.	• Mangelhafte Ereignishandhabungsverfahren, vertragliche Kontrollmechanismen und Garantien in der Dienstanbietervereinbarung, die die Abhängigkeit von Schlüsselkräften von Dritten und Verkäufern erhöhen. • Unangemessene Änderungsmanagementkontrollen in Bezug auf die IKT-Umgebung des Dienstanbieters können zu umfassenden Diensteinschränkungen oder -ausfällen führen.
	Unzureichende Sicherheit der Drittanbieter oder anderer Gruppenunter-nehmen	Gehackte IKT-Systeme der Drittanbieter mit direkten Auswirkungen auf die ausgelagerten Dienste oder beim Dienstanbieter gespeicherte kritische/vertrauliche Daten. Dienstanbieter, die einen unberechtigten Zugriff auf beim Dienstanbieter gespeicherten kritischen/sensiblen Daten erhalten	• Das Hacken von Dienstanbietern durch Kriminelle oder Terroristen als Einstiegspunkt in die IKT-Systeme der Institute oder zum Zugriff/ zur Zerstörung kritischer oder sensibler Daten, die beim Dienstanbieter gespeichert sind. • Böswillige Mitarbeiter des Dienstanbieters versuchen, sensible Daten zu stehlen und zu verkaufen.