EUROPÄISCHE
KOMMISSION

Brüssel, den 13.3.2024
C(2024) 1532 final

DELEGIERTE VERORDNUNG (EU) .../... DER KOMMISSION

vom 13.3.2024

zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens

(Text von Bedeutung für den EWR)

BEGRÜNDUNG

1. KONTEXT DES DELEGIERTEN RECHTSAKTS

Die Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA) dient unter anderem dem Ziel, einheitliche Anforderungen an die Sicherheit der Netzwerk- und Informationssysteme von im Finanzsektor tätigen Unternehmen und Organisationen festzulegen. Mit der Verordnung wird ein Rechtsrahmen für die digitale operationale Resilienz geschaffen, der alle Finanzunternehmen dazu verpflichtet sicherzustellen, dass sie jeglichen Arten von IKT-bezogenen Störungen und Bedrohungen standhalten, auf sie reagieren und den Normalbetrieb wiederherstellen können. Die betreffenden Anforderungen gelten in der gesamten EU und sollen Cyberbedrohungen verhindern und ihre Folgen eindämmen.

Gemäß Artikel 15 Unterabsatz 4 der DORA-Verordnung entwickeln die ESA „*über den Gemeinsamen Ausschuss in Abstimmung mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) gemeinsame Entwürfe technischer Regulierungsstandards*“ mit dem Ziel der „*Harmonisierung von Tools, Methoden, Prozessen und Richtlinien für IKT-Risikomanagement*“. Zudem entwickeln sie gemäß Artikel 16 einen vereinfachten IKT-Risikomanagementrahmen für bestimmte Finanzunternehmen. Dementsprechend wurde die ENISA am Gemeinsamen ESA-Unterausschusses für die digitale operationale Resilienz („JC SC DOR“) beteiligt.

Mit der vorliegenden delegierten Verordnung, die der Kommission am 17. Januar 2024 vorgelegt wurde, wird dem vorgenannten Auftrag entsprochen.

2. KONSULTATIONEN VOR ANNAHME DES RECHTSAKTS

Im Rahmen der Ausarbeitung der in diesem Verordnungsentwurf enthaltenen Standards stellten die ESA den Entwurf technischer Regulierungsstandards am 19. Juni 2023 für einen Konsultationszeitraum von drei Monaten, der am 11. September 2023 endete, zur öffentlichen Konsultation. Die ESA erhielten 120 Beiträge von unterschiedlichen Marktteilnehmern aus dem gesamten Finanzsektor. Ein vollständiger Überblick über die Beiträge der Interessenträger findet sich im Abschlussbericht der ESA[1].

Die Teilnehmer an der öffentlichen Konsultation äußerten sich zu folgenden Aspekten des vorgeschlagenen RTS-Entwurfs:

- Forderungen nach einer Verlängerung der Umsetzungsfrist,
- Forderungen nach mehr Verhältnismäßigkeit (z. B. nach Verhältnismäßigkeit in beide Richtungen, d. h. Berücksichtigung sowohl erhöhter als auch verminderter Komplexität und Risiken, und nach einem stärker sektorspezifischen Ansatz, der z. B. mehr Verhältnismäßigkeit für Versicherungsunternehmen bietet),
- Forderungen nach einem Ausschluss von Governance-Aspekten, die nicht unter das Mandat zu fallen scheinen, und
- Forderungen nach einem Verzicht auf Prüfung zusätzlicher Maßnahmen für Cloud-Computing-Ressourcen.

[1] Die Europäischen Aufsichtsbehörden (2024), „Final report on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554“.

Angesichts der eingegangenen Bemerkungen nahmen die ESA verschiedene Änderungen an den RTS-Entwürfen vor. Diese betrafen u. a. die Stärkung der Verhältnismäßigkeit, die Streichung des Artikels über Governance-Bestimmungen aus den allgemeinen Anforderungen und die Präzisierung von Bestimmungen, insbesondere in den Artikeln über Netzwerksicherheit, Verschlüsselung, Zugangskontrolle und Geschäftsfortführung. Die ESA sprachen sich gegen die Aufnahme Cloud-Computing-spezifischer Elemente aus, um dem Grundsatz der Technologieneutralität treu zu bleiben, beschlossen aber, die Anforderungen auf IKT-Assets bzw. -Dienste auszuweiten, die IKT-Drittdienstleister im Allgemeinen bereitstellen. Was die Umsetzungsfristen anbelangt, haben die ESA keine Änderungen vorgenommen, da diese Fristen auf der DORA-Ebene 1 festgelegt sind.

3. RECHTLICHE ASPEKTE DES DELEGIERTEN RECHTSAKTS

Titel I Kapitel I enthält die wichtigsten Grundsätze und Elemente, die bei der Entwicklung und Umsetzung der Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit zu berücksichtigen sind (Artikel 1).

In Titel II Kapitel II werden die Bedingungen für die weitere Harmonisierung von Tools, Methoden, Verfahren und Richtlinien für das IKT-Risikomanagement festgelegt sowie allgemeine (Abschnitt 1) und spezifische (Abschnitt 2) Elemente der Richtlinien, Verfahren, Protokolle und Tools für die IKT-Sicherheit: die Risikotoleranzschwelle, die Methoden für die Durchführung der IKT-Risikobewertung und Maßnahmen für den Umgang mit IKT-Risiken, eine Strategie für die Verwaltung von IKT-Assets (Abschnitt 3), eine Strategie für Verschlüsselung und kryptografische Kontrollen (Abschnitt 4), eine Strategie für IKT-Sicherheit (Abschnitt 5), eine Strategie für die Netzwerksicherheit (Abschnitt 6), eine Strategie für das Management von IKT-Projekten (Abschnitt 7) und eine Strategie für die physische Sicherheit und die Sicherheit vor Umweltereignissen zur Wahrung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten (Abschnitt 8). In Kapitel II werden die Elemente der IKT-Sicherheit festgelegt, die Finanzunternehmen in ihren Richtlinien für die Personalpolitik und Zugangskontrolle berücksichtigen müssen. In Kapitel III werden die Elemente der Strategie festgelegt, die Finanzunternehmen zur Erkennung IKT-bezogener Vorfälle und die Reaktion darauf entwickeln und umsetzen müssen. In Kapitel IV werden Inhalt und Format des Berichts über die Überprüfung des IKT-Risikomanagementrahmens festgelegt, den die Finanzunternehmen erstellen und vorlegen müssen.

Titel III enthält einen vereinfachten IKT-Risikomanagementrahmen mit Schwerpunkt auf Governance und Kontrolle (Kapitel I), Zugangs- und Kontrollmechanismen und -anforderungen (Kapitel II), Regelungen für die Erstellung eines IKT-Geschäftsfortführungsplans (Kapitel III) sowie für Inhalt und Format des Berichts über die Überprüfung des IKT-Risikomanagementrahmens, den die Finanzunternehmen erstellen und vorlegen müssen (Kapitel IV).

Titel IV enthält die Schlussbestimmungen über das Inkrafttreten des Rechtsakts (Artikel 42).

DELEGIERTE VERORDNUNG (EU) .../... DER KOMMISSION

vom 13.3.2024

zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011[2], insbesondere auf Artikel 15 Unterabsatz 4 und Artikel 16 Absatz 3 Unterabsatz 4,

in Erwägung nachstehender Gründe:

(1) Die Verordnung (EU) 2022/2554 gilt für ein breites Spektrum von Finanzunternehmen, die sich in Bezug auf Größe, Struktur, interne Organisation sowie Art und Komplexität ihrer Tätigkeiten unterscheiden und daher mehr oder weniger Komplexitäts- oder Risikoelemente aufweisen. Um sicherzustellen, dass dieser Vielfalt gebührend Rechnung getragen wird, sollten sämtliche Anforderungen in Bezug auf Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit sowie einen vereinfachten IKT-Risikomanagementrahmen in einem angemessenen Verhältnis zu Größe, Struktur, interner Organisation, Art und Komplexität dieser Finanzunternehmen und den damit verbundenen Risiken stehen.

(2) Aus dem gleichen Grund sollten Finanzunternehmen, die der Verordnung (EU) 2022/2554 unterliegen, bei der Erfüllung der Anforderungen an Richtlinien, Verfahren, Protokolle und Tools für die IKT-Sicherheit sowie bei einem vereinfachten IKT-Risikomanagementrahmen über eine gewisse Flexibilität verfügen. Deshalb sollten Finanzunternehmen zur Erfüllung von Dokumentationsanforderungen, die sich aus diesen Anforderungen ergeben, sämtliche Unterlagen, über die sie bereits verfügen, verwenden dürfen. Die Entwicklung, Dokumentation und Umsetzung spezifischer Richtlinien für die IKT-Sicherheit sollte nur für bestimmte wesentliche Elemente verlangt werden, wobei auch die führenden Branchenpraktiken und -normen berücksichtigt werden sollten. Um spezifische technische Aspekte der Umsetzung abzudecken, müssen entsprechende Verfahren der IKT-Sicherheit entwickelt,

[2] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

dokumentiert und umgesetzt werden, unter anderem für das Kapazitäts- und Leistungsmanagement, den Umgang mit Schwachstellen und das Patch-Management, die Daten- und Systemsicherheit sowie die Protokollierung.

(3) Um die ordnungsgemäße Umsetzung der in Titel II Kapitel I genannten Richtlinien, Verfahren, Protokolle und Tools für die IKT-Sicherheit im Zeitverlauf zu gewährleisten, ist es wichtig, dass Finanzunternehmen alle Aufgaben und Zuständigkeiten im Zusammenhang mit der IKT-Sicherheit korrekt zuweisen und aufrechterhalten und dass sie festlegen, welche Folgen die Nichteinhaltung von Richtlinien oder Verfahren der IKT-Sicherheit hat.

(4) Um das Risiko von Interessenkonflikten zu begrenzen, sollten Finanzunternehmen bei der Zuweisung von IKT-Aufgaben und -Zuständigkeiten für Aufgabentrennung sorgen.

(5) Um Flexibilität zu gewährleisten und den Kontrollrahmen der Finanzunternehmen zu vereinfachen, sollten diese nicht verpflichtet sein, spezifische Bestimmungen über die Folgen der Nichteinhaltung der in Titel II Kapitel I genannten Richtlinien, Verfahren und Protokolle für die IKT-Sicherheit auszuarbeiten, wenn solche Bestimmungen bereits im Rahmen einer anderen solchen Richtlinie oder eines anderen solchen Verfahrens festgelegt sind.

(6) In einem dynamischen Umfeld, in dem ständig neue IKT-Risiken entstehen, ist es wichtig, dass Finanzunternehmen sich bei der Entwicklung von Richtlinien für die IKT-Sicherheit auf führende Verfahren und gegebenenfalls Normen im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates[3] stützen. Dies sollte es den in Titel II genannten Finanzunternehmen ermöglichen, in einer sich wandelnden Landschaft gut informiert und vorbereitet zu sein.

(7) Zur Gewährleistung der digitalen operationalen Resilienz sollten in Titel II genannte Finanzunternehmen im Rahmen ihrer Richtlinien, Verfahren, Protokolle und Tools für die IKT-Sicherheit eine Richtlinie für das Management von IKT-Assets, Verfahren für das Kapazitäts- und Leistungsmanagement sowie Richtlinien und Verfahren für IKT-Tätigkeiten entwickeln und umsetzen. Diese Richtlinien und Verfahren sind notwendig, um die Überwachung des Status von IKT-Assets während ihres gesamten Lebenszyklus zu gewährleisten, damit sie wirksam genutzt und gepflegt werden (Management von IKT-Assets). Diese Richtlinien und Verfahren sollten zudem eine Optimierung der IKT-Systeme gewährleisten und sicherstellen, dass die Leistung und die Kapazitäten der IKT-Systeme den für Betriebs- und Informationssicherheit formulierten Zielen gerecht werden (Kapazitäts- und Leistungsmanagement). Schließlich sollten diese Richtlinien und Verfahren gewährleisten, dass das laufende Management und der laufende Betrieb der IKT-Systeme (IKT-Tätigkeiten) wirksam und reibungslos vonstattengehen, und so das Risiko eines Verlusts der Vertraulichkeit, Integrität und Verfügbarkeit von Daten minimieren. Diese Richtlinien und Verfahren sind somit erforderlich, um die Sicherheit der Netzwerke zu gewährleisten,

[3] Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012, S. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

angemessene Schutzvorkehrungen gegen Eindringen und Datenmissbrauch zu bieten und die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten zu wahren.

(8) Um einen ordnungsgemäßen Umgang mit Risiken bei IKT-Altsystemem zu gewährleisten, sollten Finanzunternehmen Fristen für die Bereitstellung von IKT-Unterstützungsdiensten durch Dritte erfassen und überwachen. Angesichts der potenziellen Auswirkungen eines Verlusts der Vertraulichkeit, Integrität und Verfügbarkeit von Daten sollten sich Finanzunternehmen bei der Erfassung und Überwachung dieser Fristen auf IKT-Assets oder -Systeme konzentrieren, die für den Geschäftsbetrieb von kritischer Bedeutung sind.

(9) Kryptografische Kontrollen können die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten gewährleisten. In Titel II genannte Finanzunternehmen sollten daher solche Kontrollen auf der Grundlage eines risikobasierten Ansatzes festlegen und durchführen. Zu diesem Zweck sollten Finanzunternehmen in einem zweistufigen Prozess Daten einstufen und IKT-Risiken umfassend bewerten und im Anschluss daran betreffende Daten, die gespeichert sind oder übermittelt werden, und erforderlichenfalls auch solche, die gerade verwendet werden, entsprechend verschlüsseln. Angesichts der Komplexität der Verschlüsselung in Verwendung befindlicher Daten sollten die in Titel II dieser Verordnung genannten Finanzunternehmen solche Daten nur verschlüsseln, wenn dies angesichts der Ergebnisse der IKT-Risikobewertung angemessen ist. Wenn die Verschlüsselung in Verwendung befindlicher Daten nicht möglich oder zu komplex ist, sollten in Titel II genannte Finanzunternehmen in der Lage sein, die Vertraulichkeit, Integrität und Verfügbarkeit der betreffenden Daten durch andere Maßnahmen für IKT-Sicherheit zu schützen. Vor dem Hintergrund der raschen technologischen Entwicklung im Bereich der Kryptografie sollten in Titel II genannte Finanzunternehmen über Entwicklungen in der Kryptoanalyse auf dem Laufenden bleiben und führende Praktiken und Normen berücksichtigen. In Titel II genannte Finanzunternehmen sollten daher einen flexiblen Ansatz verfolgen, der auf Risikominderung und -überwachung beruht, sodass sie vor dem Hintergrund der Dynamik kryptografischer Bedrohungen in der Lage sind, solche Bedrohungen, einschließlich Bedrohungen aufgrund der Fortschritte im Bereich der Quantentechnologie, zu bewältigen.

(10) Die Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit und -Betrieb sind von wesentlicher Bedeutung für die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Ein zentraler Aspekt ist dabei die strikte Trennung der IKT-Produktionsumgebungen von Entwicklungs-, Test- und anderen Nicht-Produktionsumgebungen. Diese Trennung ist eine wichtige IKT-Sicherheitsmaßnahme gegen einen unbeabsichtigten und unbefugten Zugriff auf Daten und die Änderung und Löschung von Daten in der Produktionsumgebung, die zu größeren Störungen der Geschäftstätigkeit der in Titel II genannten Finanzunternehmen führen können. Gleichwohl sollte es Finanzunternehmen angesichts der derzeitigen IKT-Entwicklungsverfahren im Ausnahmefall gestattet sein, auch in Produktionsumgebungen zu testen, sofern sie diese Tests begründen und die erforderliche Genehmigung erhalten.

(11) IKT-Landschaften, IKT-Schwachstellen und Cyberbedrohungen verändern sich ständig, sodass für die Ermittlung, Bewertung und Behebung von IKT-Schwachstellen ein proaktiver und umfassender Ansatz benötigt wird. Ohne einen solchen Ansatz drohen Finanzunternehmen, ihren Kunden, Nutzern und Gegenparteien erhebliche Risiken in Bezug auf ihre digitale operationale Resilienz, die Sicherheit ihrer

Netzwerke und die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten, die durch Richtlinien und Verfahren der IKT-Sicherheit geschützt werden sollen. Daher sollten in Titel II genannte Finanzunternehmen Schwachstellen in ihrem IKT-Umfeld ermitteln und beheben, und sowohl Finanzunternehmen als auch ihre IKT-Drittdienstleister sollten in einem Rahmen arbeiten, der einen kohärenten, transparenten und verantwortungsvollen Umgang mit Schwachstellen gewährleistet. Aus demselben Grund sollten Finanzunternehmen IKT-Schwachstellen mithilfe zuverlässiger Ressourcen und automatisierter Tools überwachen und prüfen, ob IKT-Drittdienstleister bei Schwachstellen bereitgestellter IKT-Dienste unverzüglich aktiv werden.

(12) Patch-Management sollte ein wesentlicher Bestandteil dieser IKT-Sicherheitsrichtlinien und -verfahren sein, die dazu dienen, durch Erprobung und Einführung in einer kontrollierten Umgebung festgestellte Schwachstellen zu beseitigen und Störungen durch die Installation von Patches zu verhindern.

(13) Um im Hinblick auf potenzielle Sicherheitsbedrohungen, die für das Finanzunternehmen und seine Interessenträger relevant sein könnten, eine zeitnahe und transparente Kommunikation zu gewährleisten, sollten Finanzunternehmen Verfahren für eine verantwortungsvolle Offenlegung von IKT-Schwachstellen gegenüber Kunden, Gegenparteien und der Öffentlichkeit festlegen. Bei der Festlegung dieser Verfahren sollten Finanzunternehmen verschiedene Faktoren berücksichtigen und zum Beispiel prüfen, wie schwerwiegend die Schwachstelle ist, wie sie sich auf die Interessenträger auswirken kann und wie schnell für Abhilfe oder eine Minderung der Auswirkungen gesorgt werden kann.

(14) Bei der Zuweisung von Zugangsrechten an Nutzer sollten in Titel II genannte Finanzunternehmen durch strenge Maßnahmen sicherstellen, dass eine eindeutige Identifizierung von Personen und Systemen, die auf die Informationen des Finanzunternehmens zugreifen, gewährleistet ist. Wird dies versäumt, so setzt sich das betreffende Finanzunternehmen dem Risiko von potenziell unbefugten Zugriffen, Datenschutzverletzungen und betrügerischen Aktivitäten und somit der Gefahr einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit sensibler Finanzdaten aus. Auch wenn die Verwendung von generischen oder gemeinsam genutzten Konten unter Umständen, die die Finanzunternehmen festlegen, ausnahmsweise zulässig sein sollte, sollten die Finanzunternehmen doch sicherstellen, dass Handlungen, die über diese Konten erfolgen, zurechenbar bleiben. Ist dies nicht der Fall, so bietet sich potenziellen böswilligen Nutzern die Möglichkeit, Ermittlungs- und Korrekturmaßnahmen zu behindern, was bei den Finanzunternehmen die Gefahr von unentdeckten böswilligen Handlungen oder von Sanktionen wegen Nichteinhaltung erhöhen würde.

(15) Angesichts der raschen Fortschritte in IKT-Umgebungen sollten die in Titel II genannten Finanzunternehmen robuste Richtlinien und Verfahren für das IKT-Projektmanagement implementieren, um die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten zu gewährleisten. In diesen Richtlinien und Verfahren für das IKT-Projektmanagement sollte festgelegt werden, welche Elemente für den Erfolg von IKT-Projekten erforderlich sind, einschließlich Änderungen, Beschaffung, Wartung und Entwicklung der IKT-Systeme des Finanzunternehmens, wobei es keine Rolle spielt, welche Methodik das Finanzunternehmen für das IKT-Projektmanagement gewählt hat. Im Rahmen dieser Richtlinien und Verfahren sollten Finanzunternehmen bedarfsgerechte Testverfahren und -methoden einführen, ohne jedoch Abstriche an ihrem risikobasierten Ansatz und einem sicheren, zuverlässigen

und resilienten IKT-Umfeld zu machen. Zur Gewährleistung einer sicheren Durchführung von IKT-Projekten sollten Finanzunternehmen sicherstellen, dass Mitarbeiter aus bestimmten Geschäftsbereichen oder Funktionen, in denen das entsprechende IKT-Projekt Wirkung zeigen wird, die erforderlichen Informationen und Fachkenntnisse bereitstellen können. Um eine wirksame Aufsicht zu gewährleisten, sollten dem Leitungsorgan Berichte über IKT-Projekte und damit verbundene Risiken vorgelegt werden, insbesondere wenn diese Projekte kritische oder wichtige Funktionen betreffen. Finanzunternehmen sollten die Häufigkeit und die Einzelheiten der systematischen und laufenden Überprüfungen und Berichte auf Bedeutung und Umfang der betreffenden IKT-Projekte abstimmen.

(16) Softwarepakete, die in Titel II genannte Finanzunternehmen erwerben und entwickeln, müssen im Einklang mit den gesetzten Zielen für Betriebs- und Informationssicherheit wirksam und sicher in das bestehende IKT-Umfeld eingebunden werden. Finanzunternehmen sollten solche Softwarepakete daher gründlich bewerten. Zu diesem Zweck und zur Ermittlung von Schwachstellen und potenziellen Sicherheitslücken in den Softwarepaketen und den umfassenderen IKT-Systemen sollten Finanzunternehmen IKT-Sicherheitstests durchführen. Um die Integrität der Software zu bewerten und sicherzustellen, dass ihre Verwendung keine Risiken für die IKT-Sicherheit birgt, sollten Finanzunternehmen auch Quellcodes erworbener Software und nach Möglichkeit von IKT-Drittanbietern bereitgestellter proprietärer Software unter Verwendung statischer und dynamischer Testmethoden überprüfen.

(17) Änderungen bergen unabhängig von ihrem Umfang bestimmte inhärente Risiken, können erhebliche Risiken für den Verlust der Vertraulichkeit, Integrität und Verfügbarkeit von Daten mit sich bringen und somit zu schwerwiegenden Betriebsstörungen führen. Um Finanzunternehmen vor potenziellen IKT-Schwachstellen und damit verbundenen erheblichen Risiken zu schützen, wird ein strenges Überprüfungsverfahren benötigt, um festzustellen, ob Änderungen die erforderlichen IKT-Sicherheitsanforderungen erfüllen. Deshalb sollten sich die in Titel II genannten Finanzunternehmen solide Richtlinien und Verfahren für das IKT-Änderungsmanagement geben und diese als wesentliches Element ihrer Richtlinien und Verfahren für die IKT-Sicherheit behandeln. Um Objektivität und Wirksamkeit des IKT-Änderungsmanagements zu wahren, Interessenkonflikte zu vermeiden und eine objektive Bewertung von IKT-Änderungen sicherzustellen, müssen die für die Genehmigung dieser Änderungen zuständigen Funktionen von den Funktionen getrennt sein, die Änderungen anstoßen und umsetzen. Zur Gewährleistung eines wirksamen Übergangs, einer kontrollierten Umsetzung von IKT-Änderungen und minimaler Störungen des Betriebs der IKT-Systeme sollten Finanzunternehmen Rollen und Zuständigkeiten eindeutig zuweisen, um sicherzustellen, dass IKT-Änderungen gut geplant und angemessen getestet werden und dass Qualität gewährleistet ist. Ferner sollten Finanzunternehmen Ausweichverfahren entwickeln und umsetzen, die gewährleisten, dass IKT-Systeme weiterhin wirksam funktionieren, und für ein Sicherheitsnetz sorgen. Finanzunternehmen sollten diese Ausweichverfahren eindeutig definieren und die entsprechenden Zuständigkeiten zuweisen, um eine rasche und wirksame Reaktion auf nicht erfolgreich verlaufene IKT-Änderungen zu gewährleisten.

(18) Mit Blick auf die Erkennung, Steuerung und Meldung IKT-bezogener Vorfälle sollten in Titel II genannte Finanzunternehmen eine Strategie für IKT-bezogene Vorfälle mit den Komponenten eines IKT-Vorfallmanagements festlegen. Zu diesem Zweck sollten Finanzunternehmen alle relevanten Kontakte inner- und außerhalb der Organisation

ermitteln, die eine ordnungsgemäße Koordinierung und Durchführung der verschiedenen Phasen dieses Prozesses unterstützen können. Zur Verbesserung der Erkennung IKT-bezogener Vorfälle und der Reaktion darauf und um bei diesen Vorfällen Trends zu ermitteln, die Finanzunternehmen wertvolle Informationen liefern können, um grundlegende Ursachen und Probleme wirksam auszumachen und anzugehen, sollten Finanzunternehmen IKT-bezogene Vorfälle und insbesondere solche, die sie unter anderem aufgrund ihres regelmäßigen Wiederauftretens für besonders wichtig halten, eingehend analysieren.

(19) Im Interesse einer frühzeitigen und wirksamen Aufdeckung von Anomalien sollten in Titel II genannte Finanzunternehmen unterschiedliche Informationsquellen erfassen, überwachen und analysieren und entsprechende Rollen und Zuständigkeiten zuweisen. Bei internen Informationsquellen sind Protokolle eine höchst relevante Quelle, doch sollten sich Finanzunternehmen nicht allein auf Protokolle verlassen. Stattdessen sollten sie umfassendere Informationen prüfen und auch Meldungen anderer interner Funktionen einbeziehen, die oft eine wertvolle Quelle relevanter Informationen sind. Aus dem gleichen Grund sollten Finanzunternehmen Informationen aus externen Quellen analysieren und überwachen, einschließlich der von IKT-Drittanbietern bereitgestellten Informationen über Vorfälle, die ihre Systeme und Netze betreffen, sowie anderer Informationsquellen, die Finanzunternehmen für relevant halten. Soweit personenbezogene Daten betroffen sind, findet das Datenschutzrecht der Union Anwendung. Die personenbezogenen Daten sollten auf das für die Erkennung des Vorfalls erforderliche Maß beschränkt sein.

(20) Zur Verbesserung der Erkennung IKT-bezogener Vorfälle sollten Finanzunternehmen diese Vorfälle dokumentieren. Um einerseits sicherzustellen, dass solche Nachweise ausreichend lang aufbewahrt werden, und andererseits einen übermäßigen Aufwand zu vermeiden, sollten Finanzunternehmen bei der Festlegung der Speicherfrist unter anderem die Kritikalität der betreffenden Daten und die sich aus dem Unionsrecht ergebenden Anforderungen an die Vorratsspeicherung berücksichtigen.

(21) Um sicherzustellen, dass IKT-bezogene Vorfälle zeitnah erkannt werden, sollten in Titel II genannte Finanzunternehmen sich nicht auf die Kriterien für die Erkennung IKT-bezogener Vorfälle und die Reaktion darauf beschränken. Finanzunternehmen sollten jedes dieser Kriterien berücksichtigen, doch sollten die Auslösung der Verfahren für die Erkennung IKT-bezogener Vorfälle und die Reaktion darauf nicht davon abhängen, dass die in den Kriterien beschriebenen Umstände gleichzeitig auftreten, und sollte die Bedeutung der betroffenen IKT-Dienste angemessen berücksichtigt werden.

(22) Bei der Entwicklung von IKT-Geschäftsfortführungsleitlinien sollten in Titel II genannte Finanzunternehmen die wesentlichen Komponenten des IKT-Risikomanagements berücksichtigen, darunter Management- und Kommunikationsstrategien für IKT-bezogene Vorfälle, Prozesse für das IKT-Änderungsmanagement und mit IKT-Drittanbietern verbundene Risiken.

(23) Es muss festgelegt werden, welche Szenarien in Titel II genannte Finanzunternehmen bei der Umsetzung ihrer IKT-Reaktions- und Wiederherstellungspläne und bei der Erprobung von IKT-Geschäftsfortführungsplänen berücksichtigen sollten. Diese Szenarien sollten den Finanzunternehmen als Ausgangspunkt für die Analyse von Relevanz und Plausibilität jedes Szenarios und der Notwendigkeit alternativer Szenarien dienen. Finanzunternehmen sollten sich auf Szenarien konzentrieren, in denen sich Investitionen in Resilienzmaßnahmen als besonders effizient und wirksam

erweisen könnten. Durch Erprobung von Umstellungen von der primären IKT-Infrastruktur auf redundante Kapazitäten, Backups und redundante Systeme sollten die Finanzinstitute prüfen, ob diese Kapazitäten, Backups und Systeme während eines ausreichend langen Zeitraums wirksam funktionieren und sicherstellen, dass der normale Betrieb der primären IKT-Infrastruktur im Einklang mit den Wiederherstellungszielen wiederaufgenommen wird.

(24) Es werden Anforderungen bezüglich des operationellen Risikos benötigt, insbesondere Anforderungen an das IKT-Projekt- und Änderungsmanagement und die IKT-Geschäftsfortführung, die auf den Anforderungen aufbauen, die gemäß den Verordnungen (EU) Nr. 648/2012[4], (EU) Nr. 600/2014[5] und (EU) Nr. 909/2014[6] des Europäischen Parlaments und des Rates bereits für zentrale Gegenparteien, Zentralverwahrer und Handelsplätze gelten.

(25) Gemäß Artikel 6 Absatz 5 der Verordnung (EU) 2022/2554 müssen Finanzunternehmen ihren IKT-Risikomanagementrahmen überprüfen und ihrer zuständigen Behörde einen Bericht über diese Überprüfung vorlegen. Damit die zuständigen Behörden die in diesen Berichten enthaltenen Informationen einfach verarbeiten können und eine angemessene Übermittlung dieser Informationen gewährleistet ist, sollten Finanzunternehmen diese Berichte in einem durchsuchbaren elektronischen Format übermitteln.

(26) Bei den Anforderungen an Finanzunternehmen, die dem in Artikel 16 der Verordnung (EU) 2022/2554 genannten vereinfachten IKT-Risikomanagementrahmen unterliegen, sollte der Schwerpunkt auf den wesentlichen Bereichen und Elementen liegen, die angesichts des Umfangs, des Risikos, der Größe und der Komplexität der betreffenden Finanzunternehmen mindestens erforderlich sind, um die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten und Dienste dieser Finanzunternehmen zu gewährleisten. Diese Finanzunternehmen sollten über einen internen Governance- und Kontrollrahmen mit klar festgelegten Zuständigkeiten verfügen, der die Grundlage für einen wirksamen und soliden Rahmen für das Risikomanagement bietet. Zur Verringerung des administrativen und operativen Aufwands sollten diese Finanzunternehmen nur eine Richtlinie entwickeln und dokumentieren, nämlich eine Richtlinie für Informationssicherheit, in der die übergeordneten Grundsätze und Vorschriften zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten und der Dienste dieser Finanzunternehmen festgelegt sind.

(27) Die Bestimmungen dieser Verordnung beziehen sich auf den IKT-Risikomanagementrahmen und legen spezifische Elemente, die gemäß Artikel 15 der Verordnung (EU) 2022/2554 für Finanzunternehmen gelten, sowie den vereinfachten IKT-Risikomanagementrahmen für die in Artikel 16 Absatz 1 der genannten Verordnung aufgeführten Finanzunternehmen fest. Um die Kohärenz zwischen dem

---

[4] Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister (ABl. L 201 vom 27.7.2012, S. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

[5] Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 173 vom 12.6.2014, S. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

[6] Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012 (ABl. L 257 vom 28.8.2014, S. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

normalen und dem vereinfachten IKT-Risikomanagementrahmen zu gewährleisten und um sicherzustellen, dass diese Bestimmungen zum gleichen Zeitpunkt anwendbar sind, ist es angezeigt, sie in einen einzigen Rechtsakt aufzunehmen.

(28) Diese Verordnung beruht auf dem Entwurf technischer Regulierungsstandards, der der Kommission von der Europäischen Bankenaufsichtsbehörde, der Europäischen Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung und der Europäischen Wertpapier- und Marktaufsichtsbehörde (Europäische Aufsichtsbehörden) in Absprache mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) vorgelegt wurde.

(29) Der in Artikel 54 der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates[7], in Artikel 54 der Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates[8] und in Artikel 54 der Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates[9] genannte Gemeinsame Ausschuss der Europäischen Aufsichtsbehörden hat zu diesem Entwurf technischer Regulierungsstandards, auf dem die vorliegende Verordnung beruht, öffentliche Konsultationen durchgeführt, die damit verbundenen Kosten- und Nutzeneffekte analysiert und die Stellungnahme der nach Artikel 37 der Verordnung (EU) Nr. 1093/2010 eingesetzten Interessengruppe Bankensektor, der nach Artikel 37 der Verordnung (EU) Nr. 1094/2010 eingesetzten Interessengruppe Versicherung und Rückversicherung und der nach Artikel 37 der Verordnung (EU) Nr. 1095/2010 eingesetzten Interessengruppe Wertpapiere und Wertpapiermärkte eingeholt.

(30) Soweit zur Erfüllung der in diesem Rechtsakt festgelegten Verpflichtungen die Verarbeitung personenbezogener Daten erforderlich ist, sollten die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 und die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 uneingeschränkt Anwendung finden. Wenn beispielsweise personenbezogene Daten erhoben werden, um eine angemessene Erkennung von Vorfällen zu gewährleisten, sollte der Grundsatz der Datenminimierung eingehalten werden. Der Europäische Datenschutzbeauftragte wurde zum Entwurf dieses Rechtsakts konsultiert —

HAT FOLGENDE VERORDNUNG ERLASSEN:

---

7 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

8 Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

9 Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

TITEL I
ALLGEMEINER GRUNDSATZ

Artikel 1
Gesamtrisikoprofil und -komplexität

Bei der Entwicklung und Implementierung der Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit nach Titel II und des vereinfachten IKT-Risikomanagementrahmens nach Titel III werden Größe und Gesamtrisikoprofil des Finanzunternehmens sowie die Art und der Umfang seiner Dienstleistungen, Tätigkeiten und Geschäfte und die Elemente berücksichtigt, die deren Komplexität erhöhen oder verringern, darunter:

a) Verschlüsselung und Kryptografie;

b) IKT-Betriebssicherheit;

c) Netzwerksicherheit;

d) IKT-Projekt- und -Änderungsmanagement;

e) die potenziellen Auswirkungen des IKT-Risikos auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowie von Störungen, die die Kontinuität und Verfügbarkeit der Tätigkeiten des Finanzunternehmens beeinträchtigen.

TITEL II
WEITERE HARMONISIERUNG VON TOOLS, METHODEN, PROZESSEN UND RICHTLINIEN FÜR IKT-RISIKOMANAGEMENT IM EINKLANG MIT ARTIKEL 15 DER VERORDNUNG (EU) 2022/2554

KAPITEL I
RICHTLINIEN, VERFAHREN, PROTOKOLLE UND TOOLS FÜR IKT-SICHERHEIT

ABSCHNITT 1

Artikel 2
Allgemeine Elemente der Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit

(1) Die Finanzunternehmen stellen sicher, dass ihre IKT-Sicherheitsrichtlinien, die Informationssicherheit und die damit verbundenen Verfahren, Protokolle und Tools nach Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 in ihren IKT-Risikomanagementrahmen eingebettet sind. Die Finanzunternehmen legen Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit nach diesem Kapitel fest, die

a) die Netzwerksicherheit gewährleisten;

b) Schutzvorkehrungen gegen Eindringen und Missbrauch von Daten umfassen;

c) die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten wahren, einschließlich durch den Einsatz kryptografischer Techniken;

d) eine präzise und rasche Datenübermittlung ohne wesentliche Störungen und unangemessene Verzögerungen gewährleisten.

(2) Die Finanzunternehmen stellen sicher, dass die in Absatz 1 genannten IKT-Sicherheitsrichtlinien

a) auf die Ziele für die Informationssicherheit des Finanzunternehmens abgestimmt sind, die in der in Artikel 6 Absatz 8 der Verordnung (EU) 2022/2554 genannten Strategie für die digitale operationale Resilienz enthalten sind;

b) das Datum der förmlichen Genehmigung der IKT-Sicherheitsrichtlinien durch das Leitungsorgan enthalten;

c) Indikatoren und Maßnahmen für Folgendes umfassen:

i) Überwachung der Implementierung der Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit,

ii) Erfassung von Ausnahmen von dieser Implementierung,

iii) Gewährleistung, dass bei Ausnahmen im Sinne von Ziffer ii die digitale operationale Resilienz des Finanzunternehmens sichergestellt ist;

d) die Verantwortlichkeiten der Mitarbeiter auf allen Ebenen festlegen, um die IKT-Sicherheit des Finanzunternehmens zu gewährleisten;

e) die Folgen einer Nichteinhaltung der IKT-Sicherheitsrichtlinien durch Mitarbeiter des Finanzunternehmens spezifizieren, sofern einschlägige Bestimmungen nicht in anderen Richtlinien des Finanzunternehmens enthalten sind;

f) ein Verzeichnis der erforderlichen Dokumentation umfassen;

g) die Regelungen für die Aufgabentrennung nach dem Modell der drei Verteidigungslinien oder gegebenenfalls einem anderen internen Modell für Risikomanagement und Kontrolle spezifizieren, um Interessenkonflikte zu vermeiden;

h) führende Praktiken und gegebenenfalls Normen im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 berücksichtigen;

i) die Aufgaben und Verantwortlichkeiten für die Entwicklung, Implementierung und Aufrechterhaltung von Richtlinien, Verfahren, Protokollen und Tools für IKT-Sicherheit festlegen;

j) im Einklang mit Artikel 6 Absatz 5 der Verordnung (EU) 2022/2554 überprüft werden;

k) wesentliche Änderungen in Bezug auf das Finanzunternehmen, einschließlich wesentlicher Änderungen der Tätigkeiten oder Prozesse des Finanzunternehmens, der Cyberbedrohungslage oder der geltenden rechtlichen Verpflichtungen, berücksichtigen.

ABSCHNITT 2

Artikel 3
IKT-Risikomanagement

Die Finanzunternehmen entwickeln, dokumentieren und implementieren Richtlinien und Verfahren für das IKT-Risikomanagement, die alle folgenden Elemente umfassen:

a) einen Verweis auf die Genehmigung der nach Artikel 6 Absatz 8 Buchstabe b der Verordnung (EU) 2022/2554 festgelegten Risikotoleranzschwelle für IKT-Risiken;

b) ein Verfahren und eine Methodik für die Durchführung der IKT-Risikobewertung, um Folgendes zu ermitteln:

   i) Schwachstellen und Bedrohungen, die die unterstützten Unternehmensfunktionen, die IKT-Systeme und die IKT-Assets, die diese Funktionen unterstützen, beeinträchtigen oder beeinträchtigen könnten,

   ii) die quantitativen oder qualitativen Indikatoren zur Messung der Auswirkungen und der Wahrscheinlichkeit eines Auftretens der unter Ziffer i genannten Schwachstellen und Bedrohungen;

c) das Verfahren zur Ermittlung, Implementierung und Dokumentation von Maßnahmen für die Behandlung von IKT-Risiken mit Blick auf die ermittelten und bewerteten IKT-Risiken, einschließlich der Festlegung von Maßnahmen für die Behandlung von IKT-Risiken, die erforderlich sind, um diese unter die Risikotoleranzschwelle nach Buchstabe a zu senken;

d) für IKT-Restrisiken, die nach der Implementierung der Maßnahmen für die Behandlung von IKT-Risiken gemäß Buchstabe c weiter bestehen:

i) Bestimmungen über die Ermittlung dieser IKT-Restrisiken,

ii) die Zuweisung von Aufgaben und Verantwortlichkeiten mit Blick auf

(1) das Eingehen von IKT-Restrisiken, die die Risikotoleranzschwelle nach Buchstabe a des Finanzunternehmens überschreiten,

(2) das Überprüfungsverfahren gemäß Buchstabe d Ziffer iv,

iii) die Erstellung eines Inventars der eingegangenen IKT-Restrisiken, einschließlich einer Begründung, weshalb sie eingegangen wurden,

iv) Bestimmungen über die Überprüfung der eingegangenen IKT-Restrisiken, die mindestens einmal jährlich vorgenommen wird, einschließlich zur

(1) Ermittlung etwaiger Änderungen der IKT-Restrisiken,

(2) Bewertung der verfügbaren Abhilfemaßnahmen,

(3) Bewertung, ob die Gründe für das Eingehen der IKT-Restrisiken zum Zeitpunkt der Überprüfung noch gültig und anwendbar sind;

e) Bestimmungen über die Überwachung

i) jeglicher Änderungen der IKT-Risiken und der Cyberbedrohungslage,

ii) interner und externer Schwachstellen und Bedrohungen,

iii) des IKT-Risikos des Finanzunternehmens, damit Änderungen, die sich auf sein IKT-Risikoprofil auswirken könnten, rasch erkannt werden können;

f) Bestimmungen über ein Verfahren, mit dem sichergestellt wird, dass alle Änderungen der Geschäftsstrategie und der Strategie für die digitale operationale Resilienz des Finanzunternehmens berücksichtigt werden.

Für die Zwecke von Absatz 1 Buchstabe c stellt das dort genannte Verfahren sicher, dass

a) die Wirksamkeit der implementierten Maßnahmen für die Behandlung von IKT-Risiken überwacht wird;

b) bewertet wird, ob die festgelegten Risikotoleranzschwellen des Finanzunternehmens erreicht wurden;

c) bewertet wird, ob das Finanzunternehmen tätig geworden ist, um diese Maßnahmen erforderlichenfalls zu korrigieren oder zu verbessern.

ABSCHNITT 3
MANAGEMENT VON IKT-ASSETS

Artikel 4
Richtlinie für das Management von IKT-Assets

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools eine Richtlinie für das Management von IKT-Assets.

(2) Die in Absatz 1 genannte Richtlinie für das Management von IKT-Assets enthält

a) Vorschriften für die Überwachung und das Management des Lebenszyklus von IKT-Assets, die gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 ermittelt und klassifiziert werden;

b) Vorschriften, wonach das Finanzunternehmen in seinen Aufzeichnungen Folgendes erfasst:

i) die eindeutige Kennung jedes IKT-Assets,

ii) Informationen über den physischen oder logischen Standort aller IKT-Assets,

iii) die Klassifizierung aller IKT-Assets gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2254,

iv) die Identität der Eigentümer von IKT-Assets,

v) die Unternehmensfunktionen oder -dienstleistungen, die durch das IKT-Asset unterstützt werden,

vi) die für die IKT-Geschäftsfortführung geltenden Anforderungen, einschließlich der Vorgaben für die Wiederherstellungszeit und die Wiederherstellungspunkte,

vii) die Möglichkeit eines Zugriffs auf das IKT-Asset über externe Netzwerke, einschließlich des Internets,

viii) die Verbindungen und Interdependenzen zwischen IKT-Assets und den Unternehmensfunktionen, die die einzelnen IKT-Assets nutzen,

ix) für alle IKT-Assets gegebenenfalls die Fristen bis zum Ende des Zeitraums, in dem die regelmäßigen, erweiterten und kundenspezifischen Unterstützungsdienstleistungen des IKT-Drittdienstleisters bereitgestellt werden und nach dem diese IKT-Assets nicht mehr von ihrem Anbieter oder einem IKT-Drittdienstleister unterstützt werden;

c) Vorschriften für Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, wonach diese Finanzunternehmen Aufzeichnungen über die Informationen führen, die für die Durchführung einer spezifischen IKT-Risikobewertung aller IKT-Altsysteme nach Artikel 8 Absatz 7 der Verordnung (EU) 2022/2554 erforderlich sind.

Artikel 5
Verfahren für das Management von IKT-Assets

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren ein Verfahren für das Management von IKT-Assets.

(2) In dem in Absatz 1 genannten Verfahren für das Management von IKT-Assets werden die Kriterien festgelegt, nach denen die Bewertung der Kritikalität von Informationsassets und IKT-Assets, die Unternehmensfunktionen unterstützen, vorgenommen wird. Bei dieser Bewertung wird Folgendes berücksichtigt:

a) das IKT-Risiko im Zusammenhang mit diesen Unternehmensfunktionen und deren Abhängigkeit von den Informationsassets oder IKT-Assets;

b) mögliche Auswirkungen des Verlusts der Vertraulichkeit, Integrität und Verfügbarkeit solcher Informationsassets und IKT-Assets auf die Geschäftsprozesse und -tätigkeiten der Finanzunternehmen.

ABSCHNITT 4
VERSCHLÜSSELUNG UND KRYPTOGRAFIE

Artikel 6
Verschlüsselung und kryptografische Kontrollen

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools eine Richtlinie für Verschlüsselung und kryptografische Kontrollen.

(2) Die Finanzunternehmen konzipieren die in Absatz 1 genannte Richtlinie für Verschlüsselung und kryptografische Kontrollen auf der Grundlage der Ergebnisse einer genehmigten Datenklassifizierung sowie der IKT-Risikobewertung. Diese Richtlinie enthält Vorschriften zu allen folgenden Aspekten:

a) Verschlüsselung von Daten, die gespeichert sind oder gerade übermittelt werden;

b) Verschlüsselung von Daten, die gerade verwendet werden, soweit erforderlich;

c) Verschlüsselung der internen Netzwerkverbindungen und der Datenübermittlungen mit externen Parteien;

d) Management kryptografischer Schlüssel nach Artikel 7, um die Regeln für die korrekte Verwendung, den Schutz und den Lebenszyklus kryptografischer Schlüssel festzulegen.

Ist eine Verschlüsselung gerade verwendeter Daten nicht möglich, verarbeiten die Finanzunternehmen für die Zwecke von Buchstabe b gerade verwendete Daten in einer getrennten und geschützten Umgebung oder ergreifen gleichwertige Maßnahmen, um die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der Daten zu gewährleisten.

(3) Die Finanzunternehmen nehmen in die in Absatz 1 genannte Richtlinie für Verschlüsselung und kryptografische Kontrollen Kriterien für die Auswahl kryptografischer Techniken und Nutzungspraktiken auf, wobei führende Praktiken und Normen im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 sowie die Klassifizierung einschlägiger IKT-Assets gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 zu berücksichtigen sind. Finanzunternehmen, die nicht in der Lage sind, die führenden Praktiken oder Normen einzuhalten oder die zuverlässigsten Techniken anzuwenden, ergreifen Abhilfe- und Überwachungsmaßnahmen, die die Resilienz gegenüber Cyberbedrohungen gewährleisten.

(4) Die Finanzunternehmen nehmen in die in Absatz 1 genannte Richtlinie für Verschlüsselung und kryptografische Kontrollen Bestimmungen auf, in denen geregelt ist, wie die kryptografische Technologie aufgrund von Entwicklungen im Bereich der Kryptoanalyse gegebenenfalls zu aktualisieren oder zu ändern ist. Mit solchen Aktualisierungen oder Änderungen wird sichergestellt, dass die kryptografische Technologie nach Maßgabe von Artikel 10 Absatz 2 Buchstabe a gegen Cyberbedrohungen resilient bleibt. Finanzunternehmen, die nicht in der Lage sind, die kryptografische Technologie zu aktualisieren oder zu ändern, ergreifen Abhilfe- und Überwachungsmaßnahmen, die die Resilienz gegenüber Cyberbedrohungen sicherstellen.

(5) Die Finanzunternehmen nehmen in die in Absatz 1 genannte Richtlinie für Verschlüsselung und kryptografische Kontrollen eine Anforderung auf, nach der die Annahme von Abhilfe- und Überwachungsmaßnahmen im Einklang mit den Absätzen 3 und 4 aufzuzeichnen und zu begründen ist.

Artikel 7
Management kryptografischer Schlüssel

(1) Die Finanzunternehmen nehmen in die in Artikel 6 Absatz 2 Buchstabe d genannte Richtlinie für das Management kryptografischer Schlüssel Anforderungen auf, die für das Management kryptografischer Schlüssel über ihren gesamten Lebenszyklus hinweg gelten, einschließlich mit Blick auf die Generierung, Erneuerung, Speicherung, Sicherung, Archivierung, den Abruf, die Übermittlung, Rücknahme, den Widerruf und die Vernichtung dieser kryptografischen Schlüssel.

(2) Die Finanzunternehmen ermitteln und implementieren Kontrollen, um kryptografische Schlüssel während ihres gesamten Lebenszyklus vor Verlust, unbefugtem Zugriff, Offenlegung und Änderung zu schützen. Die Finanzunternehmen konzipieren diese Kontrollen auf der Grundlage der Ergebnisse der genehmigten Datenklassifizierung und der IKT-Risikobewertung.

(3) Die Finanzunternehmen entwickeln und implementieren Methoden, um die kryptografischen Schlüssel im Verlustfall oder bei Beeinträchtigungen oder Beschädigungen dieser Schlüssel auszutauschen.

(4) Die Finanzunternehmen erstellen und führen für mindestens diejenigen IKT-Assets, die kritische oder wichtige Funktionen unterstützen, ein Register aller Zertifikate und Zertifikatspeicher. Die Finanzunternehmen halten dieses Register auf dem neuesten Stand.

(5) Die Finanzunternehmen stellen sicher, dass die Zertifikate vor Ablauf unverzüglich erneuert werden.

ABSCHNITT 5
IKT-BETRIEBSSICHERHEIT

Artikel 8
Richtlinien und Verfahren für IKT-Vorgänge

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools Richtlinien und Verfahren für das Management der IKT-Vorgänge. In diesen Richtlinien und Verfahren wird festgelegt, wie Finanzunternehmen ihre IKT-Assets betreiben, überwachen, kontrollieren und wiederherstellen, einschließlich der Dokumentation der IKT-Vorgänge.

(2) Die in Absatz 1 genannten Richtlinien und Verfahren für IKT-Vorgänge enthalten alle folgenden Elemente:

a) eine Beschreibung der IKT-Assets, einschließlich aller folgenden Elemente:

i) Anforderungen an die sichere Installation, Wartung, Konfiguration und Deinstallation eines IKT-Systems,

ii) Anforderungen an das Management von Informationsassets, die von IKT-Assets genutzt werden, einschließlich ihrer automatisierten und manuellen Verarbeitung und Behandlung,

iii) Anforderungen an die Ermittlung und Kontrolle von IKT-Altsystemen;

b) Kontrollen und Überwachung für IKT-Systeme, einschließlich aller folgenden Elemente:

i) Anforderungen an die Sicherung und Wiederherstellung von IKT-Systemen,

ii) Anforderungen an zeitliche Abläufe unter Berücksichtigung der Interdependenzen zwischen den IKT-Systemen,

iii) Protokolle für Prüfpfad- und Systemprotokollinformationen,

iv) Anforderungen, mit denen sichergestellt wird, dass bei der Durchführung einer internen Prüfung und anderer Tests Störungen des Geschäftsbetriebs minimiert werden,

v) Anforderungen an die Trennung von IKT-Produktionsumgebungen von Entwicklungs-, Test- und anderen Nicht-Produktionsumgebungen,

vi) Anforderungen hinsichtlich der Durchführung von Entwicklungs- und Testtätigkeiten in Umgebungen, die von der Produktionsumgebung getrennt sind,

vii) Anforderungen im Zusammenhang mit Situationen, in denen die Entwicklungs- und Testtätigkeiten in Produktionsumgebungen durchgeführt werden;

c) Fehlerbehandlung bei IKT-Systemen, einschließlich aller folgenden Elemente:

i) Verfahren und Protokolle für die Fehlerbehandlung,

ii) Unterstützung und Ansprechpartner im Eskalationsfall, einschließlich externer Ansprechpartner für die Unterstützung im Falle unerwarteter operationaler oder technischer Probleme,

iii) Verfahren für den Neustart, das Zurücksetzen und die Wiederherstellung von IKT-Systemen im Falle einer Störung des IKT-Systems.

Für die Zwecke von Buchstabe b Ziffer v werden bei der Trennung alle Komponenten der Umgebung berücksichtigt, einschließlich Konten, Daten oder Verbindungen, wie in Artikel 13 Absatz 1 Buchstabe a festgelegt.

Für die Zwecke von Buchstabe b Ziffer vii ist in den in Absatz 1 genannten Richtlinien und Verfahren vorzusehen, dass die Fälle, in denen Tests in einer Produktionsumgebung durchgeführt werden, eindeutig zu identifizieren, zu begründen und zeitlich zu begrenzen sind und von der betreffenden Funktion im Einklang mit Artikel 16 Absatz 6 genehmigt werden. Die Finanzunternehmen stellen während der Entwicklungs- und Testtätigkeiten in der Produktionsumgebung die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität von IKT-Systemen und -Produktionsdaten sicher.

Artikel 9
Kapazitäts- und Leistungsmanagement

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools Verfahren für das Kapazitäts- und Leistungsmanagement, die Folgendes betreffen:

a) die Ermittlung der Anforderungen an die Kapazität ihrer IKT-Systeme,

b) die Anwendung von Methoden zur Ressourcenoptimierung,

c) Überwachungsverfahren, um Folgendes aufrechtzuerhalten und zu verbessern:

i) die Verfügbarkeit von Daten und IKT-Systemen,

ii) die Effizienz der IKT-Systeme,

iii) die Verhinderung von IKT-Kapazitätsengpässen.

(2) Durch die in Absatz 1 genannten Verfahren für das Kapazitäts- und Leistungsmanagement wird sichergestellt, dass die Finanzunternehmen geeignete Maßnahmen ergreifen, um den Besonderheiten von IKT-Systemen mit langen oder komplexen Beschaffungs- oder Genehmigungsverfahren oder von ressourcenintensiven IKT-Systemen Rechnung zu tragen.

Artikel 10
Schwachstellen- und Patch-Management

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools Verfahren für das Schwachstellen-Management.

(2) Die in Absatz 1 genannten Verfahren für das Schwachstellen-Management sorgen dafür, dass

a) relevante und vertrauenswürdige Informationsressourcen ermittelt und aktualisiert werden, um für Schwachstellen zu sensibilisieren und das Bewusstsein dafür aufrechtzuerhalten,

b) die Durchführung automatisierter Schwachstellenbewertungen und -scans bei IKT-Assets gewährleistet und dabei sichergestellt wird, dass deren Häufigkeit und Umfang der im Einklang mit Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 festgelegten Klassifizierung und dem Gesamtrisikoprofil des IKT-Assets entsprechen,

c) überprüft wird, ob

i) IKT-Drittdienstleister Schwachstellen angehen, die im Zusammenhang mit den IKT-Dienstleistungen für das Finanzunternehmen stehen,

ii) diese Dienstleister dem Finanzunternehmen zumindest die kritischen Schwachstellen und Statistiken und Trends zeitnah melden;

d) nachverfolgt wird, wie Folgendes verwendet wird:

i) Bibliotheken Dritter, einschließlich Open-Source-Bibliotheken, die für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen genutzt werden,

ii) IKT-Dienstleistungen, die das Finanzunternehmen selbst entwickelt hat oder von einem IKT-Drittdienstleister speziell für das Finanzunternehmen angepasst oder entwickelt wurden;

e) Verfahren für die verantwortungsvolle Offenlegung von Schwachstellen gegenüber Kunden, Gegenparteien und der Öffentlichkeit festgelegt werden,

f) die Einführung von Patches und anderen Abhilfemaßnahmen priorisiert wird, um die ermittelten Schwachstellen zu beheben,

g) die Behebung von Schwachstellen überwacht und geprüft wird,

h) eine Aufzeichnung aller festgestellten Schwachstellen, die IKT-Systeme betreffen, und die Überwachung der Behebung dieser Schwachstellen verlangt werden.

Für die Zwecke von Buchstabe b führen die Finanzunternehmen die automatisierten Schwachstellenbewertungen und -scans für IKT-Assets bei IKT-Assets, die kritische oder wichtige Funktionen unterstützen, mindestens einmal wöchentlich durch.

Für die Zwecke von Buchstabe c fordern die Finanzunternehmen IKT-Drittdienstleister auf, die einschlägigen Schwachstellen zu untersuchen, die Ursachen zu ermitteln und geeignete Abhilfemaßnahmen zu ergreifen.

Für die Zwecke von Buchstabe d überwachen die Finanzunternehmen, gegebenenfalls in Zusammenarbeit mit dem IKT-Drittdienstleister, die aktuelle Version der Bibliotheken Dritter sowie mögliche Aktualisierungen. Was gebrauchsfertige (Standard-)IKT-Assets oder Komponenten von IKT-Assets betrifft, die für die Ausführung von IKT-Dienstleistungen erworben und verwendet werden, die keine kritischen oder wichtigen Funktionen unterstützen, wird die Nutzung von Bibliotheken Dritter, einschließlich Open-Source-Bibliotheken, von den Finanzunternehmen soweit wie möglich nachverfolgt.

Für die Zwecke von Buchstabe f berücksichtigen die Finanzunternehmen die Kritikalität der Schwachstelle, die im Einklang mit Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 festgelegte Klassifizierung sowie das Risikoprofil der IKT-Assets, die von den ermittelten Schwachstellen betroffen sind.

(3) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools Verfahren für das Patch-Management.

(4) Die in Absatz 3 genannten Verfahren für das Patch-Management dienen dazu,

a) soweit möglich verfügbare Software- und Hardware-Patches und -Aktualisierungen mithilfe automatisierter Tools zu ermitteln und zu bewerten;

b) Notfallverfahren für das Patching und die Aktualisierung von IKT-Assets zu ermitteln;

c) Software- und Hardware-Patches und die Aktualisierungen gemäß Artikel 8 Absatz 2 Buchstabe b Ziffern v, vi und vii zu testen und einzuführen;

d) Fristen für die Installation von Software- und Hardware-Patches und von Aktualisierungen zu setzen sowie Eskalationsverfahren für den Fall festzulegen, dass diese Fristen nicht eingehalten werden können.

Artikel 11
Daten- und Systemsicherheit

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools ein Verfahren für die Daten- und Systemsicherheit.

(2) Das in Absatz 1 genannte Verfahren für die Daten- und Systemsicherheit umfasst alle folgenden Elemente im Zusammenhang mit der Daten- und IKT-Systemsicherheit im Einklang mit der gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 festgelegten Klassifizierung:

a) die in Artikel 21 dieser Verordnung genannten Zugangsbeschränkungen zur Unterstützung der Anforderungen im Zusammenhang mit dem Schutz für jede Klassifizierungsstufe;

b) die Ermittlung von Mindestanforderungen an eine sichere Konfigurationsbasis für IKT-Assets, durch die die Exposition dieser IKT-Assets gegenüber Cyberbedrohungen minimiert wird, sowie Maßnahmen zur regelmäßigen Überprüfung, ob diese Mindestanforderungen wirksam verwendet werden;

c) die Ermittlung von Sicherheitsmaßnahmen, um zu gewährleisten, dass ausschließlich zugelassene Software in IKT-Systemen und Endgeräten installiert wird;

d) die Ermittlung von Sicherheitsmaßnahmen gegen Schadprogramme;

e) die Ermittlung von Sicherheitsmaßnahmen, um zu gewährleisten, dass ausschließlich zugelassene Datenträger, Systeme und Endgeräte für die Übermittlung und Speicherung von Daten des Finanzunternehmens verwendet werden;

f) die folgenden Anforderungen, um die sichere Nutzung tragbarer Endgeräte und privater nicht tragbarer Endgeräte zu gewährleisten:

   i) die Anforderung einer Lösung für das Management der Endgeräte und die Löschung von Daten des Finanzunternehmens durch Fernzugriff,

   ii) die Anforderung, Sicherheitsmechanismen zu verwenden, die von den Mitarbeitern oder IKT-Drittdienstleistern nicht auf unbefugte Weise geändert, entfernt oder umgangen werden können,

   iii) die Anforderung, mobile Datenspeicher nur dann zu verwenden, wenn das IKT-Restrisiko unter der in Artikel 3 Absatz 1 Buchstabe a genannten Risikotoleranzschwelle des Finanzunternehmens liegt;

g) das Verfahren zur sicheren Löschung von Daten in den Räumlichkeiten des Finanzunternehmens oder von extern gespeicherten Daten, die das Finanzunternehmen nicht mehr erheben oder speichern muss;

h) das Verfahren zur sicheren Entsorgung oder Außerbetriebnahme von Datenspeichern in den Räumlichkeiten des Finanzunternehmens oder von extern aufbewahrten Datenspeichern, die vertrauliche Informationen enthalten;

i) die Ermittlung und Implementierung von Sicherheitsmaßnahmen zur Verhinderung von Datenverlust und Datenlecks bei Systemen und Endgeräten;

j) die Implementierung von Sicherheitsmaßnahmen, um zu gewährleisten, dass Telearbeit und die Nutzung privater Endgeräte nicht die IKT-Sicherheit des Finanzunternehmens beeinträchtigen;

k) für IKT-Assets oder -Dienstleistungen, die von einem IKT- Drittdienstleister betrieben werden, die Ermittlung und Umsetzung von Anforderungen an die Aufrechterhaltung der digitalen operationalen Resilienz im Einklang mit den Ergebnissen der Datenklassifizierung und der IKT-Risikobewertung.

Für die Zwecke von Buchstabe b werden im Rahmen der dort genannten sicheren Konfigurationsbasis die führenden Praktiken und geeigneten Techniken berücksichtigt, die in den Normen im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 festgelegt sind.

Für die Zwecke von Buchstabe k berücksichtigen Finanzunternehmen Folgendes:

a) die Implementierung der vom Anbieter empfohlenen Einstellungen für Komponenten, die vom Finanzunternehmen betrieben werden;

b) eine klare Aufteilung der die Informationssicherheit betreffenden Aufgaben und Verantwortlichkeiten zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister im Einklang mit dem in Artikel 28 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten Grundsatz der vollen Verantwortlichkeit des Finanzunternehmens für seinen IKT-Drittdienstleister und für Finanzunternehmen nach Artikel 28 Absatz 2 der genannten Verordnung sowie im Einklang mit der Richtlinie des Finanzunternehmens für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen;

c) die Notwendigkeit, innerhalb des Finanzunternehmens angemessene Kompetenzen für das Management und die Sicherheit der in Anspruch genommenen Dienstleistungen sicherzustellen und aufrechtzuerhalten;

d) technische und organisatorische Maßnahmen zur Minimierung der Risiken im Zusammenhang mit der Infrastruktur, die der IKT-Drittdienstleister für seine IKT-Dienstleistungen nutzt, unter Berücksichtigung führender Praktiken und Normen im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012.

Artikel 12
Datenaufzeichnung

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der Schutzvorkehrungen gegen Eindringen und Missbrauch von Daten Verfahren, Protokolle und Tools für die Datenaufzeichnung.

(2) Die in Absatz 1 genannten Verfahren, Protokolle und Tools für die Datenaufzeichnung umfassen alle folgenden Elemente:

a) die Ermittlung der aufzuzeichnenden Ereignisse, die Speicherfrist für die Datenaufzeichnungen und die Maßnahmen zur Sicherung und Verarbeitung der Aufzeichnungsdaten unter Berücksichtigung des Zwecks, für den die Datenaufzeichnungen erstellt werden;

b) die Abstimmung des Detaillierungsgrads der Datenaufzeichnungen auf deren Zweck und Verwendung, um die wirksame Erkennung anomaler Aktivitäten nach Artikel 24 zu ermöglichen;

c) die Anforderung, Ereignisse aufzuzeichnen, die sämtliche der folgenden Aspekte betreffen:

   i) logische und physische Zugangskontrolle nach Artikel 21 und Identitätsmanagement,

   ii) Kapazitätsmanagement,

   iii) Änderungsmanagement,

   iv) IKT-Vorgänge, einschließlich IKT-Systemaktivitäten,

   v) Netzwerkverkehrsaktivitäten, einschließlich der Leistung der IKT-Netzwerke;

d) Maßnahmen zum Schutz von Datenaufzeichnungssystemen und -informationen vor Manipulation, Löschung und unbefugtem Zugriff mit Blick auf gespeicherte, übermittelte oder gegebenenfalls gerade verwendete Daten;

e) Maßnahmen zur Erkennung eines Ausfalls von Datenaufzeichnungssystemen;

f) unbeschadet etwaiger im Unionsrecht oder nationalen Recht festgelegter anwendbarer rechtlicher Anforderungen die Synchronisierung der Uhren jedes IKT-Systems des Finanzunternehmens auf der Grundlage einer dokumentierten zuverlässigen Referenzzeitquelle.

Für die Zwecke von Buchstabe a legen die Finanzunternehmen die Speicherfrist fest und tragen dabei den Geschäftszielen und den Zielen für die Informationssicherheit, dem Grund, weshalb das Ereignis aufgezeichnet wurde, und den Ergebnissen der IKT-Risikobewertung Rechnung.

ABSCHNITT 6
NETZWERKSICHERHEIT

Artikel 13
Management der Netzwerksicherheit

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der Schutzvorkehrungen, die die Sicherheit der Netzwerke gegen Eindringen und Missbrauch von Daten gewährleisten, Richtlinien, Verfahren, Protokolle und Tools für das Management der Netzwerksicherheit, in denen alle folgenden Aspekte behandelt werden:

a) die Trennung und Segmentierung von IKT-Systemen und -Netzwerken unter Berücksichtigung

   i) der Kritikalität oder Bedeutung der Funktion, die von diesen IKT-Systemen und -Netzwerken unterstützt wird,

   ii) der im Einklang mit Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 festgelegten Klassifizierung,

   iii) des Gesamtrisikoprofils der IKT-Assets, die diese IKT-Systeme und -Netzwerke nutzen;

b) die Dokumentation aller Netzwerkverbindungen und Datenflüsse des Finanzunternehmens;

c) die Nutzung eines gesonderten und speziellen Netzwerks für die Verwaltung von IKT-Assets;

d) die Ermittlung und Implementierung von Kontrollen für den Netzwerkzugang, um Verbindungen zum Netzwerk des Finanzunternehmens durch ein nicht zugelassenes Gerät oder System oder einen Endpunkt, der die Sicherheitsanforderungen des Finanzunternehmens nicht erfüllt, zu verhindern und zu erkennen;

e) die Verschlüsselung von Netzwerkverbindungen über Unternehmensnetzwerke, öffentliche Netzwerke, inländische Netzwerke, Netzwerke Dritter und drahtlose Netzwerke für die verwendeten Kommunikationsprotokolle unter Berücksichtigung der Ergebnisse der genehmigten Datenklassifizierung, der Ergebnisse der IKT-Risikobewertung und der Verschlüsselung von Netzwerkverbindungen gemäß Artikel 6 Absatz 2;

f) die Konzeption der Netzwerke im Einklang mit den vom Finanzunternehmen festgelegten IKT-Sicherheitsanforderungen unter Berücksichtigung führender Praktiken zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks;

g) die Sicherung des Netzwerkverkehrs zwischen den internen Netzwerken und dem Internet und anderen externen Verbindungen;

h) die Ermittlung der Aufgaben und Verantwortlichkeiten sowie der Etappen für die Spezifikation, Implementierung, Genehmigung, Änderung und Überprüfung der Firewall-Regeln und Verbindungsfilter;

i) die Überprüfung der Netzwerkarchitektur und des Konzepts für die Netzwerksicherheit einmal jährlich und für Kleinstunternehmen in regelmäßigen Abständen, um potenzielle Schwachstellen zu ermitteln;

j) die Maßnahmen zur vorübergehenden Isolierung von Teilnetzwerken sowie von Netzwerkkomponenten und -geräten, soweit erforderlich;

k) die Implementierung einer sicheren Konfigurationsbasis für alle Netzwerkkomponenten und die Absicherung des Netzwerks und der Netzwerkgeräte im Einklang mit etwaigen Anweisungen des Anbieters und gegebenenfalls mit Normen im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 sowie führenden Praktiken;

l) die Verfahren zur Begrenzung, Sperrung und Beendigung von System- und Fernsitzungen nach einer bestimmten Inaktivitätszeit;

m) für Vereinbarungen über Netzwerkdienstleistungen:

   i) die Ermittlung und Spezifikation von IKT- und Informationssicherheitsmaßnahmen, der Dienstleistungsgüte und von Managementanforderungen für alle Netzwerkdienste;

   ii) die Feststellung, ob diese Dienstleistungen von einem gruppeninternen IKT-Dienstleister oder von IKT-Drittdienstleistern erbracht werden.

Für die Zwecke von Buchstabe h überprüfen die Finanzunternehmen regelmäßig die Firewall-Regeln und die Verbindungsfilter im Einklang mit der gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 festgelegten Klassifizierung und dem Gesamtrisikoprofil der beteiligten IKT-Systeme. Bei IKT-Systemen, die kritische oder wichtige Funktionen unterstützen, überprüfen Finanzunternehmen mindestens alle sechs Monate, ob die bestehenden Firewall-Regeln und Verbindungsfilter angemessen sind.

Artikel 14
Sicherung von Informationen bei der Übermittlung

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der Schutzvorkehrungen zur Wahrung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten Richtlinien, Verfahren, Protokolle und Tools zum Schutz von Informationen, die übermittelt werden. Die Finanzunternehmen gewährleisten insbesondere Folgendes:

a) die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten während der Übermittlung über das Netzwerk und die Festlegung von Verfahren, um zu bewerten, ob diese Anforderungen eingehalten werden;

b) die Verhinderung und Erkennung von Datenlecks und die sichere Übertragung von Informationen zwischen dem Finanzunternehmen und externen Parteien;

c) die Implementierung, Dokumentation und regelmäßige Überprüfung der Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, die dem Bedarf des Finanzunternehmens hinsichtlich des Schutzes von Informationen im Zusammenhang mit den Mitarbeitern des Finanzunternehmens und Dritten Rechnung tragen.

(2) Die Finanzunternehmen konzipieren die Richtlinien, Protokolle und Tools zum Schutz von Informationen bei der Übermittlung nach Absatz 1 auf der Grundlage der Ergebnisse einer genehmigten Datenklassifizierung und der IKT-Risikobewertung.

ABSCHNITT 7
IKT-PROJEKT- UND -ÄNDERUNGSMANAGEMENT

Artikel 15
IKT-Projektmanagement

(1) Im Rahmen der Schutzvorkehrungen zur Wahrung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten entwickeln, dokumentieren und implementieren die Finanzunternehmen Richtlinien für das IKT-Projektmanagement.

(2) In den in Absatz 1 genannten Richtlinien für das IKT-Projektmanagement werden die Elemente festgelegt, die ein wirksames Management der IKT-Projekte in Bezug auf die Beschaffung, die Wartung sowie gegebenenfalls die Entwicklung der IKT-Systeme des Finanzunternehmens gewährleisten.

(3) Die in Absatz 1 genannten Richtlinien für das IKT-Projektmanagement müssen alles Folgende beinhalten:

a) die Ziele des IKT-Projekts,

b) die Governance des IKT-Projekts, samt Aufgaben und Zuständigkeiten,

c) die Planung, den zeitlichen Rahmen und die Etappen des IKT-Projekts,

d) eine IKT-Projektrisikobewertung,

e) die relevanten Etappenziele,

f) die Anforderungen an das Änderungsmanagement,

g) das Testen aller Anforderungen, einschließlich der Sicherheitsanforderungen, und das zugehörige Genehmigungsverfahren bei der Einführung eines IKT-Systems in der Produktionsumgebung.

(4) Durch Bereitstellung der erforderlichen Informationen und Fachkenntnisse aus dem Geschäftsbereich oder den geschäftlichen Funktionen, auf die sich das IKT-Projekt auswirkt, gewährleisten die in Absatz 1 genannten Richtlinien für das IKT-Projektmanagement die sichere Durchführung des Projekts.

(5) Der in Absatz 3 Buchstabe d genannten IKT-Projektrisikobewertung entsprechend müssen die in Absatz 1 genannten Richtlinien für das IKT-Projektmanagement vorsehen, dass das Leitungsorgan wie folgt über die Einleitung von IKT-Projekten, die sich auf kritische oder wichtige Funktionen des Finanzunternehmens auswirken, deren Fortschritte und die damit verbundenen Risiken unterrichtet wird:

a) einzeln oder zusammengefasst, je nach Bedeutung und Umfang der IKT-Projekte,

b) in regelmäßigen Abständen sowie erforderlichenfalls bei einzelnen Ereignissen.

Artikel 16

Beschaffung, Entwicklung und Wartung von IKT-Systemen

(1) Im Rahmen der Schutzvorkehrungen zur Wahrung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten entwickeln, dokumentieren und implementieren die Finanzunternehmen Richtlinien für die Beschaffung, die Entwicklung und die Wartung von IKT-Systemen. Diese Richtlinien müssen

a) Sicherheitskonzepte und Methoden für die Beschaffung, Entwicklung und Wartung von IKT-Systemen enthalten,

b) verlangen, dass Folgendes angegeben wird:

i) die technischen Spezifikationen und technischen IKT-Spezifikationen im Sinne von Artikel 2 Nummern 4 und 5 der Verordnung (EU) Nr. 1025/2012,

ii) die Anforderungen für die Beschaffung, die Entwicklung und die Wartung von IKT-Systemen mit besonderem Schwerpunkt auf den Anforderungen an die IKT-Sicherheit und auf deren Genehmigung durch die betreffende Geschäftsfunktion und den IKT-Asset-Eigentümer gemäß den internen Governance-Regelungen des Finanzunternehmens;

c) Maßnahmen vorsehen, mit denen das Risiko einer unbeabsichtigten Veränderung oder einer vorsätzlichen Manipulation der IKT-Systeme während der Entwicklung, Wartung und Einführung dieser IKT-Systeme in der Produktionsumgebung gemindert wird.

(2) Die Finanzunternehmen entwickeln, dokumentieren und implementieren für die Tests und die Genehmigung aller IKT-Systeme vor ihrer Nutzung und nach ihrer

Wartung gemäß Artikel 8 Absatz 2 Buchstabe b Ziffern v, vi und vii ein Verfahren für die Beschaffung, die Entwicklung und die Wartung von IKT-Systemen. Der Testumfang muss der Kritikalität der betreffenden Geschäftsprozesse und IKT-Assets angemessen sein. Die Tests müssen so ausgelegt sein, dass überprüft werden kann, ob neue IKT-Systeme ihrer geplanten Bestimmung angemessen sind, was auch die Qualität der intern entwickelten Software einschließt.

Zentrale Gegenparteien beziehen in die Ausgestaltung und Durchführung der in Unterabsatz 1 genannten Tests neben den in Unterabsatz 1 genannten Anforderungen soweit relevant die folgenden Parteien ein:

a) Clearingmitglieder und Kunden,

b) interoperable zentrale Gegenparteien,

c) andere interessierte Parteien.

Zentralverwahrer beziehen in die Ausgestaltung und Durchführung der in Unterabsatz 1 genannten Tests neben den in Unterabsatz 1 genannten Anforderungen soweit relevant die folgenden Parteien ein:

a) Nutzer,

b) kritische Versorgungsbetriebe und kritische Dienstleister,

c) andere Zentralverwahrer,

d) andere Marktinfrastrukturen,

e) alle sonstigen Institute, mit denen die Zentralverwahrer laut ihrer Geschäftsfortführungsleitlinie wechselseitige Abhängigkeiten verbinden.

(3) Im Rahmen des in Absatz 2 genannten Verfahrens sind Quellcodeprüfungen durchzuführen, die sowohl statische als auch dynamische Tests umfassen. Bei diesen Tests muss die Sicherheit internetexponierter Systeme und Anwendungen gemäß Artikel 8 Absatz 2 Buchstabe b Ziffern v, vi und vii getestet werden. Finanzunternehmen müssen

a) Schwachstellen und Anomalien im Quellcode ermitteln und analysieren,

b) einen Aktionsplan festlegen, um diese Schwachstellen und Anomalien zu beheben,

c) die Umsetzung dieses Aktionsplans überwachen.

(4) Im Rahmen des in Absatz 2 genannten Verfahrens muss spätestens zur Integrationsphase die Sicherheit von Softwarepaketen gemäß Artikel 8 Absatz 2 Buchstabe b Ziffern v, vi und vii getestet werden.

(5) Das in Absatz 2 genannte Verfahren muss Folgendes vorsehen:

a) in Nichtproduktionsumgebungen dürfen nur anonymisierte, pseudonymisierte oder randomisierte Produktionsdaten gespeichert werden,

b) Finanzunternehmen müssen die Integrität und Vertraulichkeit von Daten in Nichtproduktionsumgebungen schützen.

(6) Abweichend von Absatz 5 kann das in Absatz 2 genannte Verfahren vorsehen, dass Produktionsdaten nur für bestimmte Testanlässe, für begrenzte Zeiträume und nach Genehmigung durch die betreffende Funktion sowie nach Meldung solcher Anlässe an die IKT-Risikomanagement-Funktion gespeichert werden.

(7) Das in Absatz 2 genannte Verfahren muss Kontrollen zum Schutz der Integrität des Quellcodes von IKT-Systemen vorsehen, die intern oder von einem IKT-Drittdienstleister entwickelt und dem Finanzunternehmen von einem IKT-Drittdienstleister geliefert werden.

(8) Das in Absatz 2 genannte Verfahren muss vorsehen, dass proprietäre Software und nach Möglichkeit der Quellcode, der von IKT-Drittdienstleistern bereitgestellt wird oder aus Open-Source-Projekten stammt, vor ihrer Einführung in der Produktionsumgebung gemäß Absatz 3 analysiert und getestet werden.

(9) Die Absätze 1 bis 8 gelten auch für IKT-Systeme, die von nicht bei der IKT-Funktion angesiedelten Nutzern nach einem risikobasierten Ansatz entwickelt oder betrieben werden.

Artikel 17
IKT-Änderungsmanagement

(1) Im Rahmen der Schutzvorkehrungen zur Wahrung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten sehen die Finanzunternehmen in den in Artikel 9 Absatz 4 Buchstabe e der Verordnung (EU) 2022/2554 genannten IKT-Änderungsmanagementverfahren für alle Änderungen an Software, Hardware, Firmware-Komponenten, Systemen oder Sicherheitsparametern alles Folgende vor:

a) eine Überprüfung, ob die IKT-Sicherheitsanforderungen erfüllt sind,

b) Mechanismen, die gewährleisten, dass die Funktionen, die Änderungen genehmigen, und die Funktionen, die für die Beantragung und Umsetzung dieser Änderungen zuständig sind, unabhängig sind,

c) eine klare Beschreibung der Aufgaben und Zuständigkeiten, um zu gewährleisten, dass

   i) Änderungen angegeben und geplant werden,

   ii) ein angemessener Übergang vorgesehen ist,

   iii) die Änderungen kontrolliert getestet und finalisiert werden,

   iv) eine wirksame Qualitätssicherung gewährleistet ist,

d) die Dokumentation und Kommunikation der Änderungen im Detail, wozu u. a. Folgendes zählt:

   i) Zweck und Umfang der Änderung,

   ii) Zeitplan für die Umsetzung der Änderung,

   iii) die erwarteten Ergebnisse;

e) die Angabe von Ausweichverfahren und -zuständigkeiten, einschließlich Verfahren und Zuständigkeiten für den Abbruch von Änderungen oder die Wiederherstellung, wenn Änderungen nicht erfolgreich implementiert wurden,

f) Verfahren, Protokolle und Tools für den Umgang mit Notfalländerungen, die angemessene Schutzvorkehrungen vorsehen,

g) Verfahren zur Dokumentation, Neubewertung, Bewertung und Genehmigung von Notfalländerungen, nachdem diese vorgenommen wurden, einschließlich Ausweichlösungen und Patches,

h) Angabe der potenziellen Auswirkungen einer Änderung auf bestehende IKT-Sicherheitsmaßnahmen und Bewertung, ob eine solche Änderung zusätzliche IKT-Sicherheitsmaßnahmen erfordert.

(2) Wenn zentrale Gegenparteien und Zentralverwahrer an ihren IKT-Systemen erhebliche Änderungen vorgenommen haben, unterziehen sie diese strengen Tests unter Simulation von Stressbedingungen.

Zentrale Gegenparteien beziehen in die Ausgestaltung und Durchführung der in Unterabsatz 1 genannten Tests soweit relevant die folgenden Parteien ein:

a) Clearingmitglieder und Kunden,

b) interoperable zentrale Gegenparteien,

c) andere interessierte Parteien.

Zentralverwahrer beziehen in die Ausgestaltung und Durchführung der in Unterabsatz 1 genannten Tests soweit relevant die folgende Parteien ein:

a) Nutzer,

b) kritische Versorgungsbetriebe und kritische Dienstleister,

c) andere Zentralverwahrer,

d) andere Marktinfrastrukturen,

e) alle sonstigen Institute, mit denen die Zentralverwahrer laut ihrer IKT-Geschäftsfortführungsleitlinie wechselseitige Abhängigkeiten verbinden.

ABSCHNITT 8

Artikel 18
Physische Sicherheit und Sicherheit vor Umweltereignissen

(1) Im Rahmen der Schutzvorkehrungen zur Wahrung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten verfassen, dokumentieren und implementieren die Finanzunternehmen Richtlinien für die physische Sicherheit und die Sicherheit vor Umweltereignissen. Die Finanzunternehmen gestalten diese Richtlinien unter Berücksichtigung der Cyberbedrohungslage gemäß der nach Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 vorgenommenen Klassifizierung und unter Berücksichtigung des Gesamtrisikoprofils der IKT-Assets und der zugänglichen Informationsassets.

(2) Die in Absatz 1 genannten Richtlinien für die physische Sicherheit und die Sicherheit vor Umweltereignissen müssen alles Folgende beinhalten:

a) einen Verweis auf den Abschnitt der Richtlinien, in dem es um die in Artikel 21 Absatz 1 Buchstabe g genannte Kontrolle der Zugangs- und Zugriffsrechte geht,

b) die Maßnahmen, mit denen die Räumlichkeiten und Rechenzentren des Finanzunternehmens und die vom Finanzunternehmen designierten sensiblen Bereiche, in denen IKT- und Informationsassets untergebracht sind, vor Angriffen, Unfällen und Umweltbedrohungen und -gefahren geschützt werden,

c) die Maßnahmen, mit denen die IKT-Assets inner- und außerhalb der Räumlichkeiten des Finanzunternehmens unter Berücksichtigung der Ergebnisse der IKT-Risikobewertung für diese IKT-Assets gesichert werden,

d) Maßnahmen, mit denen die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von IKT-Assets, Informationsassets und Einrichtungen für die physische Zugangskontrolle des Finanzunternehmens durch angemessene Wartung sichergestellt werden soll,

e) Maßnahmen, mit denen die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten gewahrt werden sollen, einschließlich

   i) der Vorgabe eines „leeren Schreibtischs“,

   ii) der Vorgabe eines „leeren Bildschirms“ bei Datenverarbeitungsanlagen.

Für die Zwecke des Buchstabens b müssen die Maßnahmen zum Schutz vor Umweltbedrohungen und -gefahren der Bedeutung der Räumlichkeiten, der Rechenzentren und der designierten sensiblen Bereiche und der Kritikalität der dort untergebrachten Geschäftstätigkeiten oder IKT-Systeme angemessen sein.

Für die Zwecke des Buchstabens c müssen die in Absatz 1 genannten Richtlinien für die physische Sicherheit und die Sicherheit vor Umweltereignissen angemessene Schutzmaßnahmen für unbeaufsichtigte IKT-Assets enthalten.

Kapitel II
RICHTLINIEN FÜR PERSONALPOLITIK UND ZUGANGSKONTROLLE

Artikel 19
Richtlinien für Personalpolitik

Die Finanzunternehmen nehmen in ihre Richtlinien für Personalpolitik oder in ihre anderen einschlägigen Richtlinien alle nachstehend genannten IKT-sicherheitsbezogenen Elemente auf:

a) die Angabe und Zuweisung etwaiger spezifischer Zuständigkeiten im Bereich der IKT-Sicherheit,

b) die Vorgabe für die Mitarbeiter des Finanzunternehmens und des IKT-Drittdienstleisters, die IKT-Assets des Finanzunternehmens nutzen oder auf diese zugreifen,

   i) sich über die Richtlinien, Verfahren und Protokolle des Finanzunternehmens zur IKT-Sicherheit zu informieren und diese einzuhalten,

   ii) auf dem Laufenden darüber zu sein, welche Kanäle das Finanzunternehmen für die Meldung anomaler Verhaltensweisen geschaffen hat, wozu – soweit relevant – die gemäß der Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates[10] eingerichteten Meldekanäle zählen,

   iii) dem Finanzunternehmen nach Beendigung des Beschäftigungsverhältnisses alle in ihrem Besitz befindlichen IKT-Assets und materiellen Informationsassets, die Eigentum des Finanzunternehmens sind, auszuhändigen.

[10] Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (ABl. L 305 vom 26.11.2019, S. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

Artikel 20
Identitätsmanagement

(1) Um die Zuweisung der Nutzerzugriffsrechte gemäß Artikel 21 zu ermöglichen, entwickeln, dokumentieren und implementieren die Finanzunternehmen im Rahmen der Kontrolle der Zugangs- und Zugriffsrechte Richtlinien und Verfahren für das Identitätsmanagement, die die eindeutige Identifizierung und Authentifizierung der natürlichen Personen und Systeme, die auf Informationen der Finanzunternehmen zugreifen, gewährleisten.

(2) Die in Absatz 1 genannten Richtlinien für das Identitätsmanagement müssen alles Folgende vorsehen:

a) unbeschadet des Artikels 21 Absatz 1 Buchstabe c ist jedem Mitarbeiter des Finanzunternehmens oder Mitarbeitern der IKT-Drittdienstleister, die auf die Informationsassets und IKT-Assets des Finanzunternehmens zugreifen, eine eindeutige Identität zuzuweisen, die einem eindeutigen Nutzerkonto zugeordnet werden kann,

b) einen Lebenszyklusmanagementprozess für Identitäten und Konten, der die Erstellung, Änderung, Überprüfung und Aktualisierung, die vorübergehende Deaktivierung und die Beendigung aller Konten umfasst.

Für die Zwecke des Buchstabens a führen die Finanzunternehmen Aufzeichnungen über alle zugeordneten Identitäten. Diese Aufzeichnungen werden unbeschadet der im geltenden Unionsrecht und im nationalen Recht festgelegten Speicherpflichten nach einer Umstrukturierung des Finanzunternehmens oder nach Ablauf der Vertragsbeziehung aufbewahrt.

Für die Zwecke des Buchstabens b greifen die Finanzunternehmen beim Lebenszyklusmanagementprozess für Identitäten soweit möglich und angemessen auf automatisierte Lösungen zurück.

Artikel 21
Zugangskontrolle

Im Rahmen der Kontrolle der Zugangs- und Zugriffsrechte entwickeln, dokumentieren und implementieren die Finanzunternehmen Richtlinien, die alles Folgende vorsehen:

a) die Zuweisung der Rechte auf Zugang zu IKT-Assets nach dem Grundsatz „Kenntnis nur, wenn nötig“ („Need-to-know“), nach dem Grundsatz der Nutzungsnotwendigkeit („Need-to-use“) und nach dem Grundsatz der minimalen Berechtigung („Least privileges“), auch für den Fern- und Notfallzugang,

b) die Abtrennung der Aufgaben, einen ungerechtfertigten Zugang zu kritischen Daten zu verhindern oder die Zuweisung einer Kombination von Zugriffsrechten zu verhindern, die zur Umgehung von Kontrollen genutzt werden können,

c) eine Bestimmung zur Zurechenbarkeit, die die Nutzung generischer und gemeinsam genutzter Nutzerkonten so weit wie möglich einschränkt und die sicherstellt, dass die in den IKT-Systemen vorgenommenen Handlungen jederzeit einem Nutzer zugeordnet werden können,

d) eine Bestimmung zur Beschränkung des Zugangs zu IKT-Assets, die Kontrollen und Tools zur Verhinderung eines unbefugten Zugangs vorsieht,

e) Kontoverwaltungsverfahren für die Gewährung, Änderung oder Entziehung von Zugangsrechten für Nutzerkonten und generische Konten, insbesondere auch für generische Administratorkonten, die alles Folgende beinhalten:

   i) die Zuweisung der Aufgaben und Zuständigkeiten für die Gewährung, Überprüfung und Entziehung von Zugangsrechten,

   ii) die Zuweisung eines bevorrechtigten Zugangs, eines Notfallzugangs und eines Administratorzugangs nach dem Grundsatz der Nutzungsnotwendigkeit oder ad hoc bei allen IKT-Systemen,

   iii) den umgehenden Entzug der Zugangsrechte bei Beendigung des Beschäftigungsverhältnisses oder wenn der Zugang nicht länger erforderlich ist,

   iv) die Aktualisierung der Zugangsrechte, wenn Änderungen notwendig sind, mindestens aber einmal jährlich bei allen IKT-Systemen mit Ausnahme derjenigen, die kritische oder wichtige Funktionen unterstützen, und mindestens alle sechs Monate bei IKT-Systemen, die kritische oder wichtige Funktionen unterstützen.

f) Authentifizierungsmethoden, die alles Folgende vorsehen:

   i) die Nutzung von Authentifizierungsmethoden ist der gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 vorgenommenen Klassifizierung und dem Gesamtrisikoprofil der IKT-Assets angemessen und trägt führenden Praktiken Rechnung,

   ii) die Nutzung starker Authentifizierungsmethoden entspricht den führenden Praktiken und Techniken für den Fernzugang zum Netz des Finanzunternehmens, für den bevorrechtigten Zugang, für den Zugang zu IKT-Assets, die kritische oder wichtige Funktionen unterstützen oder IKT-Assets, die öffentlich zugänglich sind,

g) physische Zugangskontrollen, die Folgendes einschließen:

   i) die Identifizierung und Protokollierung natürlicher Personen mit Zugangsberechtigung für Räumlichkeiten, Rechenzentren und die vom Finanzunternehmen designierten sensiblen Bereiche, in denen IKT- und Informationsassets untergebracht sind,

   ii) die Gewährung der Rechte auf physischen Zugang zu kritischen IKT-Assets nur für befugte Personen nach dem Grundsatz „Kenntnis nur, wenn nötig“ und dem Grundsatz der minimalen Berechtigung sowie ad hoc,

   iii) die Überwachung des physischen Zugangs zu Räumlichkeiten, Rechenzentren und die vom Finanzunternehmen designierten sensiblen Bereiche, in denen IKT- und/oder Informationsassets untergebracht sind,

   iv) die Überprüfung der physischen Zugangsrechte, um zu gewährleisten, dass unnötige Zugangsrechte umgehend entzogen werden.

Für die Zwecke von Buchstabe e Ziffer i legen die Finanzunternehmen die Speicherfrist fest und tragen dabei den Geschäftszielen und den Zielen für die Informationssicherheit, den Gründen für die Protokollierung des Ereignisses und den Ergebnissen der IKT-Risikobewertung Rechnung.

Für die Zwecke von Buchstabe e Ziffer ii verwenden die Finanzunternehmen für die Ausführung administrativer Aufgaben in IKT-Systemen nach Möglichkeit spezielle Konten. Für das Management des bevorrechtigten Zugangs greifen die Finanzunternehmen soweit möglich und angemessen auf automatisierte Lösungen zurück.

Für die Zwecke von Buchstabe g Ziffer i müssen die Identifizierung und Protokollierung der Bedeutung der Räumlichkeiten, der Rechenzentren und der designierten sensiblen Bereiche und der Kritikalität der dort untergebrachten Geschäftstätigkeiten oder IKT-Systeme angemessen sein.

Für die Zwecke von Buchstabe g Ziffer iii muss die Überwachung der gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 vorgenommenen Klassifizierung und der Kritikalität des Zugangsbereichs angemessen sein.

KAPITEL III
ERKENNUNG IKT-BEZOGENER VORFÄLLE UND REAKTION

Artikel 22
Richtlinien für die Behandlung IKT-bezogener Vorfälle

Im Rahmen des Mechanismus zur Erkennung anomaler Aktivitäten, worunter auch Probleme bei der Leistung von IKT-Netzwerken und IKT-bezogene Vorfälle fallen, entwickeln, dokumentieren und implementieren die Finanzunternehmen Richtlinien für IKT-bezogene Vorfälle, in deren Rahmen sie

a) den in Artikel 17 der Verordnung (EU) 2022/2554 genannten Prozess für die Behandlung IKT-bezogener Vorfälle dokumentieren,

b) eine Liste der relevanten Kontakte erstellen, die mit internen Funktionen und externen Interessenträgern, die direkt an der IKT-Betriebssicherheit beteiligt sind, unter anderem in Bezug auf Folgendes unterhalten werden:

i) die Erkennung und Überwachung von Cyberbedrohungen,

ii) die Erkennung anomaler Aktivitäten,

iii) das Schwachstellenmanagement;

c) technische, organisatorische und operative Mechanismen zur Unterstützung des Prozesses für die Behandlung IKT-bezogener Vorfälle einrichten, implementieren und betreiben, darunter auch Mechanismen, die eine rasche Erkennung anomaler Tätigkeiten und Verhaltensweisen gemäß Artikel 23 ermöglichen,

d) gemäß [Artikel [15] der Delegierten Verordnung (EU) […]/[…] der Kommission [Delegierte Verordnung der Kommission zur Klassifizierung IKT-bezogener Vorfälle][11] und gemäß allen nach Unionsrecht geltenden Speichervorschriften alle Nachweise im Zusammenhang mit IKT-bezogenen Vorfällen so lange aufbewahren, wie es für die Zwecke der Datenerhebung unbedingt erforderlich und der Kritikalität der betreffenden Unternehmensfunktionen, unterstützenden Prozesse sowie IKT- und Informationsassets angemessen ist,

[11] (OP: Bitte [Fundstelle und Titel dieser delegierten VO] einfügen)

e) Mechanismen zur Analyse bedeutender oder wiederkehrender IKT-bezogener Vorfälle und -Muster in Bezug auf Anzahl und Auftreten IKT-bezogener Vorfälle einrichten und implementieren.

Für die Zwecke des Buchstabens d bewahren die Finanzunternehmen die dort genannten Nachweise auf sichere Weise auf.

Artikel 23

Erkennung anormaler Aktivitäten und Kriterien für die Erkennung IKT-bezogener Vorfälle und die Reaktion auf solche Vorfälle

(1) Um IKT-bezogene Vorfälle und anormale Aktivitäten wirkungsvoll zu erkennen und wirkungsvoll darauf reagieren zu können. legen die Finanzunternehmen klare Aufgaben und Zuständigkeiten fest.

(2) Der in Artikel 10 Absatz 1 der Verordnung (EU) 2022/2554 genannte Mechanismus zur umgehenden Erkennung anomaler Aktivitäten, darunter auch Probleme bei der Leistung von IKT-Netzwerken und IKT-bezogene Vorfälle, muss es den Finanzunternehmen ermöglichen,

a) alles Folgende zu sammeln, zu überwachen und zu analysieren:

i) interne und externe Faktoren, darunter zumindest die gemäß Artikel 12 gesammelten Protokolle, die Informationen von Unternehmens- und IKT-Funktionen sowie alle etwaigen, von Nutzern des Finanzunternehmens gemeldeten Probleme,

ii) potenzielle interne und externe Cyberbedrohungen unter Berücksichtigung der üblicherweise von Angreifern verwendeten Szenarien und der auf Bedrohungsanalysen beruhenden Szenarien,

iii) Meldungen IKT-bezogener Vorfälle durch einen IKT-Drittdienstleister des Finanzunternehmens, die in den Systemen und Netzwerken des IKT-Drittdienstleisters entdeckt wurden und Auswirkungen auf das Finanzunternehmen haben könnten,

b) anomale Aktivitäten und Verhaltensweisen festzustellen und Tools einzusetzen, die zumindest für IKT- und Informationsassets, die kritische oder wichtige Funktionen unterstützen, Warnmeldungen generieren, die auf anomale Aktivitäten und Verhaltensweisen aufmerksam machen,

c) die unter Buchstabe b genannten Warnmeldungen zu priorisieren, damit die festgestellten IKT-bezogenen Vorfälle innerhalb der von den Finanzunternehmen festgelegten erwarteten Abwicklungszeit sowohl während als auch außerhalb der Arbeitszeiten gelöst werden können,

d) sämtliche relevanten Informationen über alle anomalen Aktivitäten und Verhaltensweisen automatisch oder manuell aufzuzeichnen, zu analysieren und auszuwerten.

Für die Zwecke des Buchstabens b beinhalten die dort genannten Tools auch solche, die nach vorab definierten Regeln automatische Warnmeldungen zur Feststellung von Anomalien generieren, die die Vollständigkeit und Integrität der Datenquellen oder gesammelten Protokolle beeinträchtigen.

(3) Die Finanzunternehmen schützen jede Aufzeichnung anomaler Aktivitäten vor Manipulation und unbefugtem Zugriff und zwar unabhängig davon, ob diese Daten gespeichert sind oder gerade übermittelt oder verwendet werden.

(4) Für jede festgestellte anomale Aktivität protokollieren die Finanzunternehmen alle relevanten Informationen, die

a) die Feststellung von Datum und Uhrzeit der anomalen Aktivität ermöglichen,

b) die Feststellung von Datum und Uhrzeit der Erkennung der anomalen Aktivität ermöglichen,

c) die Feststellung der Art der anomalen Aktivität ermöglichen.

(5) Wenn die Finanzunternehmen die in Artikel 10 Absatz 2 der Verordnung (EU) 2022/2554 genannten Erkennungs- und Reaktionsprozesse für IKT-bezogene Vorfälle auslösen, tragen sie dabei allen folgenden Kriterien Rechnung:

a) Hinweisen darauf, dass in einem IKT-System oder -Netzwerk möglicherweise eine böswillige Aktivität stattgefunden hat oder dieses IKT-System oder -Netzwerk korrumpiert sein könnte,

b) Datenverlusten, die im Hinblick auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten festgestellt wurden,

c) festgestellten schädlichen Auswirkungen auf die Transaktionen und Operationen des Finanzunternehmens,

d) der Nichtverfügbarkeit von IKT-Systemen und -Netzwerken.

(6) Für die Zwecke des Absatzes 5 tragen die Finanzunternehmen auch der Kritikalität der betroffenen Dienstleistung Rechnung.

KAPITEL IV
MANAGEMENT DER IKT-GESCHÄFTSFORTFÜHRUNG

Artikel 24
Komponenten der IKT-Geschäftsfortführungsleitlinie

(1) Die Finanzunternehmen nehmen in die in Artikel 11 Absatz 1 der Verordnung (EU) 2022/2554 genannte IKT-Geschäftsfortführungsleitlinie Folgendes auf:

a) eine Beschreibung

i) der Ziele der IKT-Geschäftsfortführungsleitlinie, darunter auch der Wechselwirkungen zwischen der IKT- und der allgemeinen Geschäftsfortführung, unter Berücksichtigung der Ergebnisse der in Artikel 11 Absatz 5 der Verordnung (EU) 2022/2554 genannten Business-Impact-Analyse,

ii) des Umfangs der Geschäftsfortführungsvorkehrungen, -pläne, -verfahren und -mechanismen samt etwaiger Beschränkungen und Ausschlüsse,

iii) des von den Geschäftsfortführungsvorkehrungen, -plänen, -verfahren und -mechanismen abzudeckenden Zeitraums,

iv) der Kriterien für die Aktivierung und Deaktivierung von IKT-Geschäftsfortführungsplänen, IKT-Reaktions- und Wiederherstellungsplänen und Krisenkommunikationsplänen;

b) Bestimmungen zu:

i) Governance und Organisation zur Umsetzung der IKT-Geschäftsfortführungsleitlinie, einschließlich Aufgaben, Zuständigkeiten und Eskalationsverfahren, wobei zu gewährleisten ist, dass ausreichende Ressourcen zur Verfügung stehen,

ii) der Abstimmung zwischen den IKT-Geschäftsfortführungsplänen und den allgemeinen Geschäftsfortführungsplänen, was zumindest alles Folgende angeht:

1. die potenziellen Ausfallszenarien, einschließlich der in Artikel 26 Absatz 2 genannten Szenarien,

2. die Ziele für die Wiederherstellung des Geschäftsbetriebs, wobei festzulegen ist, dass das Finanzunternehmen den Betrieb seiner kritischen oder wichtigen Funktionen nach einer Störung entsprechend den Vorgaben für die Wiederherstellungszeit und den Wiederherstellungspunkt wiederherstellen können muss;

iii) der Entwicklung von IKT-Geschäftsfortführungsplänen für schwerwiegende Betriebsstörungen als Teil dieser Pläne und der Priorisierung der IKT-Geschäftsfortführungsmaßnahmen nach einem risikobasierten Ansatz,

iv) Entwicklung, Tests und Überprüfung der IKT-Reaktions- und Wiederherstellungspläne gemäß den Artikeln 25 und 26,

v) der Überprüfung der Wirksamkeit umgesetzter Geschäftsfortführungsvorkehrungen, -pläne, -verfahren und -mechanismen gemäß Artikel 26,

vi) der Abstimmung der IKT-Geschäftsfortführungsleitlinie mit:

1. der in Artikel 14 Absatz 2 der Verordnung (EU) 2022/2554 genannten Kommunikationsstrategie,

2. den in Artikel 11 Absatz 2 Buchstabe e der Verordnung (EU) 2022/2554 genannten Kommunikations- und Krisenmanagementmaßnahmen.

(2) Zentrale Gegenparteien stellen zusätzlich zu den Anforderungen in Absatz 1 sicher, dass ihre IKT-Geschäftsfortführungsleitlinie

a) für ihre kritischen Funktionen eine Wiederherstellungszeit von maximal 2 Stunden vorsieht,

b) externen Verbindungen und wechselseitigen Abhängigkeiten innerhalb der Finanzinfrastrukturen Rechnung trägt, darunter Handelsplätzen, die von der zentralen Gegenpartei gecleart werden, Wertpapierliefer- und -abrechnungssystemen sowie Zahlungssystemen und Kreditinstituten, die von der zentralen Gegenpartei oder einer verbundenen zentralen Gegenpartei genutzt werden;

c) Vorkehrungen im Hinblick darauf verlangt,

i) die Fortführung kritischer oder wichtiger Funktionen der zentralen Gegenpartei ausgehend von Katastrophenszenarien sicherzustellen,

ii) einen sekundären Verarbeitungsstandort zu unterhalten, der die Fortführung kritischer oder wichtiger Funktionen der zentralen Gegenpartei in gleicher Weise wie am Primärstandort gewährleisten kann,

iii) einen sekundären Geschäftsstandort zu unterhalten oder zur sofortigen Verfügung zu haben, damit die Mitarbeiter die Dienstleistung weiter erbringen können, wenn der Primärstandort nicht verfügbar ist,

iv) die Einrichtung zusätzlicher Verarbeitungsstandorte zu erwägen, insbesondere falls die unterschiedlichen Risikoprofile des primären und des sekundären Standorts keine hinreichende Gewähr dafür bieten, dass die Ziele der zentralen Gegenpartei hinsichtlich der Geschäftsfortführung in allen Szenarien erreicht werden können.

Für die Zwecke von Buchstabe a führen die zentralen Gegenparteien Tagesabschlussprozesse und Zahlungen unter allen Umständen fristgerecht durch.

Für die Zwecke von Buchstabe c Ziffer i müssen die dort genannten Vorkehrungen die Verfügbarkeit angemessener Humanressourcen, die Höchstdauer eines Ausfalls der kritischen Funktionen, den Failover zu einem sekundären Standort und die Wiederherstellung an diesem sekundären Standort regeln.

Für die Zwecke von Buchstabe c Ziffer ii muss der dort genannte sekundäre Verarbeitungsstandort ein anderes geografisches Risikoprofil aufweisen als der Primärstandort.

(3) Zentralverwahrer stellen zusätzlich zu den Anforderungen in Absatz 1 sicher, dass ihre IKT-Geschäftsfortführungsleitlinie

a) etwaigen Verbindungen und wechselseitigen Abhängigkeiten gegenüber Nutzern, kritischen Versorgungsbetrieben und kritischen Dienstleistern, anderen Zentralverwahrern und anderen Marktinfrastrukturen Rechnung trägt,

b) verlangt, dass die Vorkehrungen für die Geschäftsfortführung vorsehen, dass die Vorgabe für die Wiederherstellungszeit für ihre kritischen oder wichtigen Funktionen maximal zwei Stunden beträgt.

(4) Handelsplätze stellen zusätzlich zu den Anforderungen in Absatz 1 sicher, dass ihre IKT-Geschäftsfortführungsleitlinie gewährleistet, dass

a) der Handel nach einer Störung innerhalb von zwei Stunden oder einer geringfügig längeren Frist wieder aufgenommen werden kann,

b) der Datenverlust bei allen IT-Diensten des Handelsplatzes nach einer Störung nahezu null beträgt.

Artikel 25
Test des IKT-Geschäftsfortführungsplans

(1) Beim Test der IKT-Geschäftsfortführungspläne gemäß Artikel 11 Absatz 6 der Verordnung (EU) 2022/2554 berücksichtigen die Finanzunternehmen ihre Business-Impact-Analyse (BIA) und die in Artikel 3 Absatz 1 Buchstabe b der vorliegenden Verordnung genannte IKT-Risikobewertung.

(2) Durch den in Absatz 1 genannten Test ihrer IKT-Geschäftsfortführungspläne beurteilen die Finanzunternehmen, ob sie die Fortführung ihrer kritischen oder wichtigen Funktionen gewährleisten können. Diese Tests müssen

a) ausgehend von Testszenarien durchgeführt werden, bei denen potenzielle Störungen simuliert werden und die eine angemessene Zahl von schwerwiegenden, aber plausiblen Szenarien umfassen,

b) gegebenenfalls Tests der von IKT-Drittanbietern erbrachten IKT-Dienstleistungen umfassen,

c) bei den in Artikel 11 Absatz 6 Unterabsatz 2 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, Szenarien für Umstellungen von der primären IKT-Infrastruktur auf die redundanten Kapazitäten, Backups und Systeme enthalten,

d) darauf ausgelegt sein, die Annahmen, auf denen die Geschäftsfortführungspläne beruhen, einschließlich der Governance-Regelungen und Krisenkommunikationspläne, infrage zu stellen,

e) Verfahren enthalten, mit denen überprüft wird, ob die Mitarbeiter der Finanzunternehmen, die IKT-Drittdienstleister, die IKT-Systeme und die IKT-Dienste angemessen auf die gemäß Artikel 26 Absatz 2 gebührend berücksichtigten Szenarien reagieren.

Für die Zwecke des Buchstabens a nehmen die Finanzunternehmen in ihre Tests stets die bei Ausarbeitung der Geschäftsfortführungspläne berücksichtigten Szenarien auf.

Für die Zwecke des Buchstabens b berücksichtigen die Finanzunternehmen in gebührendem Umfang gegebenenfalls Szenarien, in denen die Insolvenz oder der Ausfall der IKT-Drittdienstleister oder politische Risiken im Sitzland der IKT-Drittdienstleister unterstellt werden.

Für die Zwecke des Buchstabens c wird bei den Tests überprüft, ob zumindest kritische oder wichtige Funktionen für ausreichend lange Zeit angemessen aufrechterhalten werden können und ob der normale Betrieb wiederhergestellt werden kann.

(3) Zentrale Gegenparteien beziehen in die in Absatz 1 genannten Tests ihrer IKT-Geschäftsfortführungspläne neben den Anforderungen in Absatz 2 folgende Parteien ein:

a) Clearingmitglieder,

b) externe Dienstleister,

c) relevante Institute in der Finanzinfrastruktur, mit denen zentrale Gegenparteien laut ihrer Geschäftsfortführungsleitlinie wechselseitige Abhängigkeiten verbinden.

(4) Zentralverwahrer beziehen in die in Absatz 1 genannten Tests ihrer IKT-Geschäftsfortführungspläne neben den Anforderungen in Absatz 2 gegebenenfalls folgende Parteien ein:

a) die Nutzer der Zentralverwahrer,

b) kritische Versorgungsbetriebe und kritische Dienstleister,

c) andere Zentralverwahrer,

d) andere Marktinfrastrukturen,

e) alle sonstigen Institute, mit denen die Zentralverwahrer laut ihrer Geschäftsfortführungsleitlinie wechselseitige Abhängigkeiten verbinden.

(5) Die Finanzunternehmen dokumentieren die Ergebnisse der in Absatz 1 genannten Tests. Alle bei diesen Tests festgestellten Schwachstellen werden analysiert, angegangen und dem Leitungsorgan zur Kenntnis gebracht.

Artikel 26
IKT-Reaktions- und Wiederherstellungspläne

(1) Bei der Ausarbeitung der in Artikel 11 Absatz 3 der Verordnung (EU) 2022/2554 genannten IKT-Reaktions- und Wiederherstellungspläne berücksichtigen die Finanzunternehmen die Ergebnisse der Business-Impact-Analyse (BIA) des Finanzunternehmens. Diese IKT-Reaktions- und Wiederherstellungspläne müssen

a) die Bedingungen für die Aktivierung oder Deaktivierung der Pläne sowie etwaige für deren Aktivierung oder Deaktivierung geltenden Ausnahmen festlegen;

b) beschreiben, welche Maßnahmen zu ergreifen sind, um die Verfügbarkeit, Integrität, Kontinuität und Wiederherstellung zumindest der IKT-Systeme und -Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen des Finanzunternehmens sicherzustellen;

c) so konzipiert sein, dass sie den Zielen für die Wiederherstellung des Geschäftsbetriebs der Finanzunternehmen gerecht werden;

d) dokumentiert und den an der Ausführung der IKT-Reaktions- und Wiederherstellungspläne beteiligten Mitarbeitern zur Verfügung gestellt werden und im Notfall leicht zugänglich sein;

e) sowohl kurz- als auch langfristige Wiederherstellungsoptionen vorsehen, insbesondere auch die teilweise Systemwiederherstellung;

f) die Ziele der IKT-Reaktions- und Wiederherstellungspläne sowie die Bedingungen festlegen, unter denen die Durchführung dieser Pläne für erfolgreich erklärt werden kann.

Für die Zwecke von Buchstabe d legen die Finanzunternehmen die Aufgaben und Zuständigkeiten klar fest.

(2) In den in Absatz 1 genannten IKT-Reaktions- und Wiederherstellungsplänen werden relevante Szenarien genannt, insbesondere auch Szenarien mit schwerwiegenden Betriebsstörungen und erhöhter Wahrscheinlichkeit, dass Störungen auftreten. In diesen Plänen werden Szenarien ausgearbeitet, die sich auf aktuelle Informationen über Bedrohungen und auf die Lehren aus früheren Betriebsstörungen stützen. Von den Finanzunternehmen werden alle folgenden Szenarien gebührend berücksichtigt:

a) Cyberangriffe und Umstellungen von der primären IKT-Infrastruktur auf die redundanten Kapazitäten, Backups und redundanten Systeme;

b) Szenarien, in denen die Qualität der Bereitstellung einer kritischen oder wichtigen Funktion auf ein inakzeptables Niveau absinkt oder diese Funktion ganz ausfällt und in denen die potenziellen Auswirkungen der Insolvenz oder sonstiger Ausfälle eines relevanten IKT-Drittdienstleisters gebührend berücksichtigt werden;

c) teilweiser oder vollständiger Ausfall von Räumlichkeiten, insbesondere auch von Büro- und Geschäftsräumen, sowie von Rechenzentren;

d) erheblicher Ausfall von IKT-Assets oder der Kommunikationsinfrastruktur;

e) Nichtverfügbarkeit einer kritischen Anzahl von Mitarbeitern oder von Mitarbeitern, die für die Gewährleistung der Betriebskontinuität zuständig sind;

f) Auswirkungen von Ereignissen im Zusammenhang mit Klimawandel und Umweltzerstörung, Naturkatastrophen, Pandemien und physischen Angriffen, insbesondere auch durch Eindringen und Terroranschläge;

g) Angriffe durch Insider;

h) politische und soziale Instabilität, sofern relevant auch im Sitzland des IKT-Drittdienstleisters und am Standort der Datenspeicherung und -verarbeitung;

i) weitverbreitete Stromausfälle.

(3) Sind die primären Wiederherstellungsmaßnahmen möglicherweise wegen Kosten, Risiken, Logistik oder unvorhergesehener Umstände kurzfristig nicht durchführbar, so werden in den in Absatz 1 genannten IKT-Reaktions- und Wiederherstellungsplänen auch Alternativen erwogen.

(4) Im Rahmen der in Absatz 1 genannten IKT-Reaktions- und Wiederherstellungspläne werden von den Finanzunternehmen Kontinuitätsmaßnahmen geprüft und durchgeführt, um Ausfälle von IKT-Drittdienstleistern, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen des Finanzunternehmens bereitstellen, zu mindern.

KAPITEL V
BERICHT ÜBER DIE ÜBERPRÜFUNG DES IKT-RISIKOMANAGEMENTRAHMENS

Artikel 27

Format und Inhalt des Berichts über die Überprüfung des IKT-Risikomanagementrahmens

(1) Die Finanzunternehmen legen den in Artikel 6 Absatz 5 der Verordnung (EU) 2022/2554 genannten Bericht über die Überprüfung des IKT-Risikomanagementrahmens in einem durchsuchbaren elektronischen Format vor.

(2) Die Finanzunternehmen nehmen in den in Absatz 1 genannten Bericht alle folgenden Informationen auf:

a) einen einleitenden Abschnitt, der Folgendes enthält:

i) eine eindeutige Angabe des Finanzunternehmens, das Gegenstand des Berichts ist, und, sofern relevant, eine Beschreibung seiner Gruppenstruktur;

ii) eine Beschreibung des Kontexts des Berichts mit Blick auf Art, Umfang und Komplexität der Dienstleistungen, Tätigkeiten und Geschäfte des Finanzunternehmens, seine Organisation, die ermittelten kritischen Funktionen, die Strategie, die wichtigsten laufenden Projekte oder Tätigkeiten, die Beziehungen und seine Abhängigkeit von internen und per Vertrag vergebenen IKT-Dienstleistungen und -Systemen oder die Auswirkungen, die ein Totalverlust oder eine schwerwiegende Verschlechterung derartiger Systeme hinsichtlich kritischer oder wichtiger Funktionen und der Markteffizienz hätte;

iii) eine Zusammenfassung der wichtigsten Veränderungen des IKT-Risikomanagementrahmens seit dem letzten vorgelegten Bericht;

iv) eine Kurzzusammenfassung des aktuellen und auf kurze Sicht bestehenden IKT-Risikoprofils, der Bedrohungslage, der erachteten Wirksamkeit seiner Kontrollen und der Sicherheitslage des Finanzunternehmens;

b) das Datum der Genehmigung des Berichts durch das Leitungsorgan des Finanzunternehmens;

c) eine Beschreibung des Grunds für die Überprüfung des IKT-Risikomanagementrahmens nach Artikel 6 Absatz 5 der Verordnung (EU) 2022/2554;

d) das Anfangs- und Enddatum des Überprüfungszeitraums;

e) eine Angabe der für die Überprüfung verantwortlichen Funktion;

f) eine Beschreibung der wichtigsten Veränderungen und Verbesserungen des IKT-Risikomanagementrahmens seit der letzten Überprüfung;

g) eine Zusammenfassung der Ergebnisse der Überprüfung und eine detaillierte Analyse und Bewertung der Schwere der Schwächen, Mängel und Lücken des IKT-Risikomanagementrahmens im Überprüfungszeitraum;

h) eine Beschreibung der Maßnahmen zur Behebung festgestellter Schwächen, Mängel und Lücken, die alles Folgende enthält:

i) eine Zusammenfassung der Maßnahmen, die zur Behebung festgestellter Schwächen, Mängel und Lücken ergriffen wurden;

ii) ein voraussichtliches Datum für die Durchführung der Maßnahmen und Daten für die interne Kontrolle der Durchführung, einschließlich Informationen über den Stand der Durchführung dieser Maßnahmen zum Zeitpunkt der Ausarbeitung des Berichts, gegebenenfalls mit einer Erläuterung, ob die Gefahr besteht, dass Fristen nicht eingehalten werden;

iii) die zu verwendenden Tools und die Nennung der für die Durchführung der Maßnahmen verantwortlichen Funktion, wobei anzugeben ist, ob es sich um interne oder externe Tools/Instrumente und Funktionen handelt;

iv) eine Beschreibung der Auswirkungen der im Rahmen der Maßnahmen geplanten Veränderungen auf die finanziellen, personellen und materiellen Ressourcen des Finanzunternehmens, insbesondere auch auf die für die Durchführung etwaiger Korrekturmaßnahmen vorgesehenen Ressourcen;

v) gegebenenfalls Informationen über das Verfahren zur Unterrichtung der zuständigen Behörde;

vi) falls die festgestellten Schwächen, Mängel oder Lücken nicht Gegenstand von Korrekturmaßnahmen sind, eine ausführliche Erläuterung der Kriterien, die zur Analyse der Auswirkungen dieser Schwächen, Mängel oder Lücken herangezogen wurden, um das damit verbundene IKT-Restrisiko zu bewerten, sowie der Kriterien für das Eingehen des damit verbundenen Restrisikos;

i) Informationen über geplante Weiterentwicklungen des IKT-Risikomanagementrahmens;

j) Schlussfolgerungen aus der Überprüfung des IKT-Risikomanagementrahmens;

k) Informationen über frühere Überprüfungen, insbesondere auch

   i) eine Liste aller bisherigen Überprüfungen;

   ii) gegebenenfalls den Stand der Umsetzung der im letzten Bericht genannten Korrekturmaßnahmen;

   iii) falls sich die in früheren Überprüfungen vorgeschlagenen Korrekturmaßnahmen als unwirksam erwiesen oder zu unerwarteten Herausforderungen geführt haben, eine Beschreibung der Möglichkeiten für eine Verbesserung dieser Korrekturmaßnahmen oder der unerwarteten Herausforderungen;

l) die zur Ausarbeitung des Berichts herangezogenen Informationsquellen, die insbesondere auch alles Folgende beinhalten müssen:

   i) bei den in Artikel 6 Absatz 6 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, die Ergebnisse der internen Revisionen;

   ii) die Ergebnisse der Compliance-Bewertungen;

   iii) die Ergebnisse der Tests der digitalen operationalen Resilienz und gegebenenfalls die Ergebnisse der erweiterten Tests von IKT-Tools, -Systemen und -Prozessen auf Basis bedrohungsorientierter Penetrationstests (TLPT – Threat-Led Penetration Testing);

   iv) externe Quellen.

Wurde die Überprüfung nach aufsichtsrechtlichen Anweisungen oder Feststellungen, die sich aus einschlägigen Tests der digitalen operationalen Resilienz oder Auditverfahren ergeben, eingeleitet, so muss der Bericht für die Zwecke des Buchstabens c ausdrückliche Verweise auf diese Anweisungen oder Feststellungen enthalten, die Aufschluss über den Grund für die Einleitung der Überprüfung geben. Wurde die Überprüfung nach IKT-bezogenen Vorfällen eingeleitet, so muss der Bericht eine Liste aller IKT-bezogenen Vorfälle mit einer Analyse der Ursachen dieser Vorfälle enthalten.

Für die Zwecke von Buchstabe f enthält die Beschreibung eine Analyse der Auswirkungen der Veränderungen auf die Strategie für die digitale operationale Resilienz des Finanzunternehmens, auf den internen IKT-Kontrollrahmen des Finanzunternehmens und auf die IKT-Risikomanagement-Governance des Finanzunternehmens.

TITEL III – VEREINFACHTER IKT-RISIKOMANAGEMENTRAHMEN FÜR DIE IN ARTIKEL 16 ABSATZ 1 DER VERORDNUNG (EU) 2022/2554 GENANNTEN FINANZUNTERNEHMEN

KAPITEL I
Vereinfachter IKT-Risikomanagementrahmen

Artikel 28
Governance und Organisation

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen müssen über einen internen Governance- und Kontrollrahmen verfügen, der ein wirksames und umsichtiges Management von IKT-Risiken gewährleistet, um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen.

(2) Die in Absatz 1 genannten Finanzunternehmen stellen im Zuge ihres vereinfachten IKT-Risikomanagementrahmens sicher, dass ihr Leitungsorgan

a) die Gesamtverantwortung dafür trägt, dass der vereinfachte IKT-Risikomanagementrahmen im Einklang mit der Risikobereitschaft des Finanzunternehmens die Verwirklichung der Geschäftsstrategie des Finanzunternehmens ermöglicht, und sicherstellt, dass IKT-Risiken in diesem Zusammenhang berücksichtigt werden;

b) für alle IKT-bezogenen Funktionen klare Aufgaben und Zuständigkeiten festlegt;

c) die Ziele für die Informationssicherheit und die IKT-Anforderungen festlegt;

d) Folgendes genehmigt, überwacht und regelmäßig überprüft:

i) die in Artikel 30 Absatz 1 dieser Verordnung genannte Klassifizierung der Informations-Assets des Finanzunternehmens, die Liste der ermittelten Hauptrisiken sowie die Business-Impact-Analyse und die zugehörigen Richtlinien;

ii) die in Artikel 16 Absatz 1 Buchstabe f der Verordnung (EU) 2022/2554 genannten Geschäftsfortführungspläne des Finanzunternehmens sowie Gegen- und Wiederherstellungsmaßnahmen;

e) die nötigen Budgetmittel zuweist und mindestens einmal jährlich überprüft, um den Anforderungen des Finanzunternehmens an die digitale operationale Resilienz in Bezug auf alle Arten von Ressourcen gerecht werden zu können, einschließlich einschlägiger Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz sowie Vermittlung von IKT-Kompetenzen für alle Mitarbeiter;

f) die in den Kapiteln I, II und III dieses Titels enthaltenen Richtlinien und Maßnahmen festlegt und umsetzt, um das IKT-Risiko, dem das Finanzunternehmen ausgesetzt ist, zu ermitteln, zu bewerten und zu managen;

g) die notwendigen Verfahren, IKT-Protokolle und Tools ermittelt und implementiert, um sämtliche Informations- und IKT-Assets zu schützen;

h) sicherstellt, dass die Mitarbeiter des Finanzunternehmens über ausreichende Kenntnisse und Fähigkeiten entsprechend den zu managenden IKT-Risiken verfügen und diesbezüglich stets auf dem neuesten Stand gehalten werden, um die IKT-Risiken und deren Auswirkungen auf die Geschäftstätigkeit des Finanzunternehmens verstehen und bewerten zu können;

i) die Modalitäten des Meldewesens festlegt, die insbesondere auch die Häufigkeit, die Form und den Inhalt der Meldungen an das Leitungsorgan über die Informationssicherheit und die digitale operationale Resilienz regeln.

(3) Die in Absatz 1 genannten Finanzunternehmen können die Überprüfung der Einhaltung der Anforderungen für das IKT-Risikomanagement im Einklang mit den sektorspezifischen Rechtsvorschriften der Union und der Mitgliedstaaten an gruppeninterne IKT-Unternehmen oder an IKT-Drittdienstleister auslagern. Im Falle einer solchen Auslagerung bleiben die Finanzunternehmen weiterhin uneingeschränkt für die Überprüfung der Einhaltung der IKT-Risikomanagementanforderungen verantwortlich.

(4) Die in Absatz 1 genannten Finanzunternehmen sorgen für eine angemessene Trennung und die Unabhängigkeit von Kontrollfunktionen und internen Revisionsfunktionen.

(5) Die in Absatz 1 genannten Finanzunternehmen stellen sicher, dass ihr vereinfachter IKT-Risikomanagementrahmen im Einklang mit dem Revisionsplan des betreffenden Finanzunternehmens einer internen Revision durch Revisoren unterzogen wird. Die Revisoren müssen über ausreichendes Wissen und ausreichende Fähigkeiten und Fachkenntnisse im Bereich IKT-Risiken verfügen und unabhängig sein. Häufigkeit und Schwerpunkt der IKT-Revisionen müssen den IKT-Risiken des Finanzunternehmens angemessen sein.

(6) Auf der Grundlage der Ergebnisse der in Absatz 5 genannten Revision stellen die in Absatz 1 genannten Finanzunternehmen die rechtzeitige Überprüfung und Auswertung kritischer Erkenntnisse der IKT-Revision sicher.

Artikel 29
Informationssicherheitsleitlinien und -maßnahmen

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen erarbeiten, dokumentieren und implementieren im Zusammenhang mit dem vereinfachten IKT-Risikomanagementrahmen eine Informationssicherheitsleitlinie. Diese Informationssicherheitsleitlinie enthält die übergeordneten Grundsätze und Regeln zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Daten und der von diesen Finanzunternehmen erbrachten Dienstleistungen.

(2) Auf der Grundlage ihrer in Absatz 1 genannten Informationssicherheitsleitlinie legen die in Absatz 1 genannten Finanzunternehmen IKT-Sicherheitsmaßnahmen zur Minderung ihres IKT-Risikos fest und setzen diese um, einschließlich Risikominderungsmaßnahmen, die von IKT-Drittdienstleistern umgesetzt werden.

Die IKT-Sicherheitsmaßnahmen müssen alle in den Artikeln 30 bis 38 genannten Maßnahmen umfassen.

Artikel 30
Klassifizierung von Informations- und IKT-Assets

(1) Im Zuge des in Artikel 16 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten vereinfachten IKT-Risikomanagementrahmens ermitteln, klassifizieren und dokumentieren die in Absatz 1 jenes Artikels genannten Finanzunternehmen alle kritischen oder wichtigen Funktionen, die Informations- und IKT-Assets, die diese Funktionen unterstützen, und deren wechselseitige Abhängigkeiten. Die Finanzunternehmen überprüfen diese Ermittlung und Klassifizierung bei Bedarf.

(2) Die in Absatz 1 genannten Finanzunternehmen ermitteln alle kritischen oder wichtigen Funktionen, die von IKT-Drittdienstleistern unterstützt werden.

Artikel 31
IKT-Risikomanagement

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen nehmen in ihren vereinfachten IKT-Risikomanagementrahmen alles Folgende auf:

a) eine Bestimmung der Risikotoleranzschwellen für das IKT-Risiko im Einklang mit der Risikobereitschaft des Finanzunternehmens;

b) die Ermittlung und Bewertung der IKT-Risiken, denen das Finanzunternehmen ausgesetzt ist;

c) die Festlegung von Abmilderungsstrategien zumindest für die IKT-Risiken, die jenseits der Risikotoleranzschwellen des Finanzunternehmens liegen;

d) die Überwachung der Wirksamkeit der unter Buchstabe c genannten Abmilderungsstrategien;

e) die Ermittlung und Bewertung etwaiger IKT- und Informationssicherheitsrisiken, die sich aus größeren Veränderungen des IKT-Systems oder der IKT-Dienstleistungen, -Prozesse oder -Verfahren sowie aus den Testergebnissen in Bezug auf die IKT-Sicherheit und nach schwerwiegenden IKT-bezogenen Vorfällen ergeben.

(2) Die in Absatz 1 genannten Finanzunternehmen führen die IKT-Risikobewertung dem IKT-Risikoprofil der Finanzunternehmen entsprechend regelmäßig durch und dokumentieren sie.

(3) Die in Absatz 1 genannten Finanzunternehmen überwachen fortlaufend Bedrohungen und Schwachstellen, die für ihre kritischen oder wichtigen Funktionen sowie für Informations- und IKT-Assets relevant sind und überprüfen regelmäßig die Risikoszenarien, die sich auf diese kritischen oder wichtigen Funktionen auswirken.

(4) Die in Absatz 1 genannten Finanzunternehmen legen Alarmschwellen und -kriterien für die Auslösung und Einleitung von Reaktionsprozessen bei IKT-bezogenen Vorfällen fest.

Artikel 32
Physische Sicherheit und Sicherheit vor Umweltereignissen

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen ermitteln und implementieren physische Sicherheitsmaßnahmen, die ausgehend von der Bedrohungslage und entsprechend der in Artikel 30 Absatz 1

der vorliegenden Verordnung genannten Klassifizierung sowie auf Basis des Gesamtrisikoprofils der IKT-Assets und der zugänglichen Informationsassets konzipiert werden.

(2) Die in Absatz 1 genannten Maßnahmen schützen die Räumlichkeiten der Finanzunternehmen und, sofern anwendbar, die Rechenzentren von Finanzunternehmen, in denen IKT- und Informationsassets untergebracht sind, vor unbefugtem Zugriff, Angriffen und Unfällen sowie vor Umweltbedrohungen und -gefahren.

(3) Der Schutz vor Umweltbedrohungen und -gefahren muss der Bedeutung der betreffenden Räumlichkeiten und, sofern anwendbar, der Rechenzentren und der Kritikalität der dort untergebrachten Geschäftstätigkeiten oder IKT-Systeme angemessen sein.

KAPITEL II
WEITERE ELEMENTE DER SYSTEME, PROTOKOLLE UND TOOLS ZUR MINIMIERUNG DER AUSWIRKUNGEN VON IKT-RISIKEN

Artikel 33
Zugangskontrolle

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen erarbeiten, dokumentieren und implementieren Verfahren für die Kontrolle des logischen und physischen Zugangs und setzen diese Verfahren durch, überwachen sie und überprüfen sie regelmäßig. Diese Verfahren umfassen die folgenden Elemente der Kontrolle des logischen und physischen Zugangs:

a) Verwaltung der Rechte auf Zugang zu Informationsassets, IKT-Assets und den durch sie unterstützten Funktionen sowie zu kritischen Betriebsstandorten des Finanzunternehmens nach dem Grundsatz „Kenntnis nur, wenn nötig“ („Need-to-know“), nach dem Grundsatz der Nutzungsnotwendigkeit („Need-to-use“) und nach dem Grundsatz der minimalen Berechtigung („Least privileges“), auch für den Fern- und Notfallzugang;

b) Zurechenbarkeit der Nutzer, die sicherstellt, dass die Nutzer, die Handlungen in den IKT-Systemen vorgenommen haben, identifiziert werden können;

c) Kontoverwaltungsverfahren für die Gewährung, Veränderung oder Entziehung von Zugangsrechten für Nutzerkonten und generische Konten, insbesondere auch für generische Administratorkonten;

d) Authentifizierungsmethoden, die der in Artikel 30 Absatz 1 genannten Klassifizierung und dem Gesamtrisikoprofil der IKT-Assets angemessen sind und auf führenden Praktiken beruhen;

e) regelmäßige Überprüfung der Zugangsrechte und Entziehung nicht mehr benötigter Zugangsrechte.

Für die Zwecke von Buchstabe c weist das Finanzunternehmen den privilegierten Zugang, den Notfallzugang und den Administratorzugang bei allen IKT-Systemen nach dem Grundsatz der Nutzungsnotwendigkeit oder ad hoc zu und protokolliert den Zugang nach Maßgabe von Artikel 34 Absatz 1 Buchstabe f in einer Log-Datei.

Für die Zwecke von Buchstabe d wenden die Finanzunternehmen starke Authentifizierungsmethoden an, die sich auf führende Praktiken für den Fernzugriff auf das Netz der Finanzunternehmen, für den privilegierten Zugang und für den Zugang zu IKT-Assets zur Unterstützung kritischer oder wichtiger Funktionen stützen, die öffentlich verfügbar sind.

Artikel 34
IKT-Betriebssicherheit

Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen müssen im Rahmen ihrer Systeme, Protokolle und Tools sowie bei allen IKT-Assets

a) den Lebenszyklus aller IKT-Assets überwachen und managen;

b) überwachen, ob die IKT-Assets von IKT-Drittdienstleistern der Finanzunternehmen unterstützt werden, sofern anwendbar;

c) die Kapazitätsanforderungen ihrer IKT-Assets und Maßnahmen ermitteln, um die Verfügbarkeit und Effizienz der IKT-Systeme zu wahren und zu verbessern und IKT-Kapazitätsengpässen vorzubeugen, bevor sie auftreten;

d) eine automatisierte Schwachstellensuche sowie Bewertungen der IKT-Assets durchführen, die der in Artikel 30 Absatz 1 genannten Klassifizierung und dem Gesamtrisikoprofil des betreffenden IKT-Assets angemessen sind, und Patches zur Behebung ermittelter Schwachstellen installieren;

e) die mit veralteten oder nicht unterstützten IKT-Assets oder mit IKT-Altsystemen verbundenen Risiken managen;

f) Vorfälle im Zusammenhang mit der logischen und physischen Zugangskontrolle, dem IKT-Betrieb, einschließlich System- und Netzwerkverkehr, sowie dem IKT-Änderungsmanagement protokollieren;

g) Maßnahmen ermitteln und umsetzen, um Informationen über anomale Aktivitäten und anomales Verhalten bei kritischen oder wichtigen IKT-Vorgängen zu überwachen und zu analysieren;

h) Maßnahmen zur Überwachung relevanter und aktueller Informationen über Cyberbedrohungen umsetzen;

i) Maßnahmen zur Erkennung etwaiger Informationslecks, Schadcodes und anderer Sicherheitsbedrohungen sowie öffentlich bekannter Schwachstellen in Software und Hardware umsetzen und die Verfügbarkeit entsprechender neuer Sicherheitsupdates prüfen.

Für die Zwecke von Buchstabe f stimmen die Finanzunternehmen den Detaillierungsgrad der Protokolle auf deren Zweck und auf die Nutzung des IKT-Assets ab, der diese Protokolle produziert.

Artikel 35
Daten-, System- und Netzwerksicherheit

Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen entwickeln und implementieren im Rahmen ihrer Systeme, Protokolle und Tools Schutzvorrichtungen, die die Sicherheit der Netzwerke gegen Eindringen und den Missbrauch von Daten gewährleisten und die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit

der Daten wahren. Insbesondere tragen die Finanzunternehmen unter Berücksichtigung der in Artikel 30 Absatz 1 genannten Klassifizierung für alles Folgende Sorge:

a) Ermittlung und Umsetzung von Maßnahmen zum Schutz von Daten, die gerade verwendet oder übermittelt werden, sowie von Daten, die gespeichert sind;

b) Ermittlung und Umsetzung von Sicherheitsmaßnahmen für die Nutzung von Software, Datenträgern, Systemen und Endgeräten, die Daten des Finanzunternehmens übertragen und speichern;

c) Ermittlung und Umsetzung von Maßnahmen zur Verhinderung und Aufdeckung unbefugter Verbindungen mit dem Netz des Finanzunternehmens und zur Sicherung des Netzverkehrs zwischen den internen Netzwerken des Finanzunternehmens und dem Internet und anderen externen Verbindungen;

d) Ermittlung und Umsetzung von Maßnahmen zur Gewährleistung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten bei Netzwerkübertragungen;

e) ein Verfahren zur sicheren Löschung von Daten in den Räumlichkeiten oder von extern gespeicherten Daten, die das Finanzunternehmen nicht mehr erheben oder speichern muss;

f) ein Verfahren zur sicheren Entsorgung oder Außerbetriebnahme von Datenspeichern in den Räumlichkeiten oder von extern gelagerten Datenspeichern, die vertrauliche Informationen enthalten;

g) Ermittlung und Umsetzung von Maßnahmen, mit denen sichergestellt wird, dass Telearbeit und die Nutzung privater Endgeräte die Fähigkeit des Finanzunternehmens, seine kritischen Tätigkeiten angemessen, rechtzeitig und sicher auszuführen, nicht beeinträchtigen.

Artikel 36
IKT-Sicherheitstests

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen erstellen und implementieren einen Plan für IKT-Sicherheitstests, um die Wirksamkeit ihrer gemäß den Artikeln 33, 34 und 35 sowie 37 und 38 der vorliegenden Verordnung entwickelten IKT-Sicherheitsmaßnahmen zu bestätigen. Die Finanzunternehmen stellen sicher, dass in diesem Plan Bedrohungen und Schwachstellen berücksichtigt werden, die im Zuge des in Artikel 31 genannten vereinfachten IKT-Risikomanagementrahmens ermittelt wurden.

(2) Die in Absatz 1 genannten Finanzunternehmen überprüfen, bewerten und testen IKT-Sicherheitsmaßnahmen unter Berücksichtigung des Gesamtrisikoprofils der IKT-Assets des Finanzunternehmens.

(3) Die in Absatz 1 genannten Finanzunternehmen überwachen und evaluieren die Ergebnisse der Sicherheitstests und bringen ihre Sicherheitsmaßnahmen im Falle von IKT-Systemen zur Unterstützung kritischer oder wichtiger Funktionen unverzüglich entsprechend auf Stand.

Artikel 37
Beschaffung, Entwicklung und Wartung von IKT-Systemen

Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen konzipieren und implementieren, sofern angemessen, ein Verfahren für die Beschaffung,

Entwicklung und Wartung von IKT-Systemen entsprechend einem risikobasierten Ansatz. Dieses Verfahren muss

a) sicherstellen, dass die funktionalen und nichtfunktionalen Anforderungen, insbesondere auch die Anforderungen an die Informationssicherheit, von der betreffenden Unternehmensfunktion klar spezifiziert und genehmigt werden, bevor IKT-Systeme beschafft oder entwickelt werden;

b) sicherstellen, dass IKT-Systeme vor ihrer erstmaligen Nutzung und vor der Einführung von Änderungen an der Produktionsumgebung getestet und genehmigt werden;

c) Maßnahmen zur Minderung des Risikos einer unbeabsichtigten Veränderung oder einer vorsätzlichen Manipulation der IKT-Systeme während der Entwicklung und Implementierung in der Produktionsumgebung vorsehen.

Artikel 38
IKT-Projekt- und -Änderungsmanagement

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen erarbeiten, dokumentieren und implementieren ein IKT-Projektmanagementverfahren und legen die Aufgaben und Zuständigkeiten für dessen Umsetzung fest. Dieses Verfahren erstreckt sich auf alle Phasen der IKT-Projekte von ihrer Einleitung bis zu ihrem Abschluss.

(2) Die in Absatz 1 genannten Finanzunternehmen entwickeln, dokumentieren und implementieren ein Verfahren für das IKT-Änderungsmanagement, um sicherzustellen, dass alle Änderungen an IKT-Systemen auf kontrollierte Weise und mit angemessenen Schutzvorkehrungen aufgezeichnet, getestet, bewertet, genehmigt, implementiert und verifiziert werden, um die digitale operationale Resilienz des Finanzunternehmens zu wahren.

Kapitel III
MANAGEMENT DER IKT-GESCHÄFTSFORTFÜHRUNG

Artikel 39
Komponenten des IKT-Geschäftsfortführungsplans

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen erarbeiten ihre IKT-Geschäftsfortführungspläne unter Berücksichtigung der Ergebnisse der Analyse des Risikos und der potenziellen Auswirkungen von schwerwiegenden Betriebsstörungen und von Szenarien, denen ihre IKT-Assets zur Unterstützung kritischer oder wichtiger Funktionen ausgesetzt sein könnten, insbesondere auch dem Szenario eines Cyberangriffs.

(2) Die in Absatz 1 genannten IKT-Geschäftsfortführungspläne müssen

a) vom Leitungsorgan des Finanzunternehmens genehmigt sein;

b) dokumentiert und im Not- oder Krisenfall leicht zugänglich sein;

c) genügend Mittel für ihre Ausführung vorsehen;

d) die geplanten Wiederherstellungsniveaus und Zeitrahmen für die Wiederherstellung und Wiederaufnahme von Funktionen sowie die wichtigsten

internen und externen Abhängigkeiten, insbesondere auch IKT-Drittdienstleister, nennen;

e) festlegen, welche Bedingungen zur Aktivierung der IKT-Geschäftsfortführungspläne führen können und welche Maßnahmen zu ergreifen sind, um die Verfügbarkeit, Kontinuität und Wiederherstellung der IKT-Assets der Finanzunternehmen zur Unterstützung kritischer oder wichtiger Funktionen sicherzustellen;

f) die Wiedergewinnungs- und Wiederherstellungsmaßnahmen für kritische oder wichtige Geschäftsfunktionen, unterstützende Prozesse, Informationsassets und deren Interdependenzen ermitteln, um nachteilige Auswirkungen auf das Funktionieren der Finanzunternehmen zu vermeiden;

g) Verfahren und Maßnahmen für die Datensicherung vorsehen, die den Umfang der Daten, die der Sicherung unterliegen, und die Mindesthäufigkeit der Sicherung auf der Grundlage der Kritikalität der diese Daten nutzenden Funktionen festlegen;

h) Alternativen für den Fall erwägen, dass eine Wiederherstellung wegen Kosten, Risiken, Logistik oder unvorhergesehener Umstände kurzfristig nicht durchführbar sein könnte;

i) die Regelungen für die interne und externe Kommunikation, insbesondere auch Eskalationspläne, festlegen;

j) aktualisiert werden, um den Lehren aus Vorfällen, Tests, neuen Risiken und ermittelten Bedrohungen, veränderten Wiederherstellungszielen sowie größeren Veränderungen der Organisation des Finanzunternehmens und der IKT-Assets zur Unterstützung kritischer oder geschäftlicher Funktionen Rechnung zu tragen.

Für die Zwecke von Buchstabe f sehen die dort genannten Maßnahmen die Minderung von Ausfällen kritischer Drittdienstleister vor.

Artikel 40
Testen der Geschäftsfortführungspläne

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen testen ihre in Artikel 39 der vorliegenden Verordnung genannten Geschäftsfortführungspläne, insbesondere auch die dort genannten Szenarien, mindestens einmal jährlich im Hinblick auf die Sicherungs- und Wiedergewinnungsverfahren oder bei jeder größeren Veränderung des Geschäftsfortführungsplans.

(2) Die in Absatz 1 genannten Tests der Geschäftsfortführungspläne müssen zeigen, dass die in jenem Absatz genannten Finanzunternehmen in der Lage sind, die Funktionsfähigkeit ihrer Geschäftstätigkeit aufrechtzuerhalten, bis kritische Vorgänge wiederhergestellt sind, und etwaige Mängel in diesen Plänen zu erkennen.

(3) Die in Absatz 1 genannten Finanzunternehmen müssen die Ergebnisse der Tests der Geschäftsfortführungspläne dokumentieren, und etwaige bei diesen Tests festgestellte Mängel müssen analysiert, behoben und dem Leitungsorgan gemeldet werden.

KAPITEL IV
BERICHT ÜBER DIE ÜBERPRÜFUNG DES VEREINFACHTEN IKT-RISIKOMANAGEMENTRAHMENS

Artikel 41
Format und Inhalt des Berichts über die Überprüfung des vereinfachten IKT-Risikomanagementrahmens

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen legen den in Absatz 2 jenes Artikels genannten Bericht über die Überprüfung des IKT-Risikomanagementrahmens in einem durchsuchbaren elektronischen Format vor.

(2) Der in Absatz 1 genannte Bericht muss alle folgenden Informationen enthalten:

a) einen einleitenden Abschnitt, der Folgendes enthält:

i) eine Beschreibung des Kontexts des Berichts mit Blick auf Art, Umfang und Komplexität der Dienstleistungen, Tätigkeiten und Geschäfte des Finanzunternehmens, die Organisation, die ermittelten kritischen Funktionen, die Strategie, die wichtigsten laufenden Projekte oder Tätigkeiten und die Beziehungen des Finanzunternehmens sowie die Abhängigkeit des Finanzunternehmens von internen und ausgelagerten IKT-Dienstleistungen und -Systemen oder die Auswirkungen, die ein Totalverlust oder eine schwerwiegende Verschlechterung derartiger Systeme hinsichtlich kritischer oder wichtiger Funktionen und der Markteffizienz hätte;

ii) eine Kurzzusammenfassung des ermittelten aktuellen und auf kurze Sicht bestehenden IKT-Risikoprofils, der Bedrohungslage, der erachteten Wirksamkeit seiner Kontrollen und der Sicherheitslage des Finanzunternehmens;

iii) Informationen über das Gebiet, über das Bericht erstattet wird;

iv) eine Zusammenfassung der wichtigsten Veränderungen des IKT-Risikomanagementrahmens seit dem letzten Bericht;

v) eine Zusammenfassung und eine Beschreibung der Auswirkungen der wichtigsten Veränderungen des IKT-Risikomanagementrahmens seit dem letzten Bericht;

b) das Datum der Genehmigung des Berichts durch das Leitungsorgan des Finanzunternehmens, sofern anwendbar;

c) eine Beschreibung der Gründe für die Überprüfung, insbesondere auch,

i) falls die Überprüfung nach aufsichtsrechtlichen Anweisungen eingeleitet wurde: Belege für diese Anweisungen;

ii) falls die Überprüfung nach Auftreten von IKT-bezogenen Vorfällen eingeleitet wurde: die Liste aller IKT-bezogenen Vorfälle mit zugehöriger Ursachenanalyse;

d) das Anfangs- und Enddatum des Überprüfungszeitraums;

e) die für die Überprüfung zuständige Person;

f) eine Zusammenfassung der Ergebnisse und eine Eigenbewertung der Schwere der Schwächen, Mängel und Lücken, die im IKT-Risikomanagementrahmen für den Überprüfungszeitraum festgestellt wurden, einschließlich einer detaillierten Analyse derselben;

g) ermittelte Abhilfemaßnahmen zur Behebung von Schwächen, Mängeln und Lücken im vereinfachten IKT-Risikomanagementrahmen und voraussichtliches Datum für die Implementierung dieser Maßnahmen, einschließlich Folgemaßnahmen für in früheren Berichten festgestellte Schwächen, Mängel und Lücken, sofern diese Schwächen, Mängel und Lücken noch nicht behoben sind;

h) allgemeine Schlussfolgerungen zur Überprüfung des vereinfachten IKT-Risikomanagementrahmens, einschließlich weiterer geplanter Entwicklungen.

TITEL IV – SCHLUSSBESTIMMUNGEN

Artikel 42
Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 13.3.2024

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN