I

(Gesetzgebungsakte)

VERORDNUNGEN

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

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Kommission,

nach Übermittlung des Entwurfs des Gesetzgebungsaktes an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank ([1]),

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([2]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:

(1) Informations- und Kommunikationstechnologien (IKT) unterstützen im digitalen Zeitalter komplexe Systeme, die für alltägliche Aktivitäten eingesetzt werden. Sie sorgen dafür, dass Schlüsselsektoren unserer Volkswirtschaften, einschließlich des Finanzsektors, am Laufen gehalten werden, und verbessern das Funktionieren des Binnenmarkts. Die zunehmende Digitalisierung und Vernetzung verstärken auch das IKT-Risiko, das die Gesellschaft insgesamt — und insbesondere das Finanzsystem — anfälliger für Cyberbedrohungen oder IKT-Störungen macht. Während die allgegenwärtige Nutzung von IKT-Systemen und die hohe Digitalisierung und Konnektivität heute grundlegende Merkmale der Tätigkeiten von Finanzunternehmen der Union sind, muss ihre digitale Resilienz erst noch besser angegangen und in ihre allgemeinen operativen Rahmen integriert werden.

(2) Die Nutzung von IKT hat in den letzten Jahrzehnten einen derart zentralen Stellenwert bei der Erbringung von Finanzdienstleistungen erlangt, dass sie heute entscheidend zur Ausführung typischer alltäglicher Aufgaben aller Finanzunternehmen beiträgt. Auf Digitalisierung beruhen heute beispielsweise Zahlungen, die von bargeld- und papiergestützten Methoden zunehmend auf die Nutzung digitaler Lösungen verlagert wurden, sowie Wertpapierclearing und -abrechnungssysteme, elektronischer und algorithmischer Handel, Darlehens- und Finanzierungsgeschäfte, Peer-to-Peer-Finanzierung, Bonitätseinstufung, Schadensmanagement und Back-Office-

([1]) ABl. C 343 vom 26.8.2021, S. 1.
([2]) ABl. C 155 vom 30.4.2021, S. 38.
([3]) Standpunkt des Europäischen Parlaments 10. November 2022 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 28. November 2022.

Transaktionen. Auch der Versicherungssektor hat sich durch den Einsatz von IKT verändert — vom Aufkommen digitaler Versicherungsvermittler, die ihre Dienste online anbieten und mit InsurTech arbeiten, bis hin zu digitalen Versicherungsgeschäften. Das Finanzwesen ist nicht nur sektorweit weitgehend digital geworden, sondern die Digitalisierung hat auch die Verflechtungen und Abhängigkeiten innerhalb des Finanzsektors sowie von Infrastrukturen Dritter und Drittdienstleistern verstärkt.

(3) Der Europäische Ausschuss für Systemrisiken (ESRB) bekräftigte in einem Bericht aus dem Jahr 2020 über systemische Cyberrisiken, wie das bestehende hohe Maß an Verflechtungen zwischen Finanzunternehmen, Finanzmärkten und Finanzmarktinfrastrukturen und insbesondere die gegenseitigen Abhängigkeiten ihrer IKT-Systeme eine Systemanfälligkeit herbeiführen könnten, da lokalisierte Cybervorfälle in einem der rund 22 000 Finanzunternehmen der Union über geografische Grenzen hinweg rasch auf das gesamte Finanzsystem übergreifen könnten. Schwerwiegende IKT-Sicherheitsverletzungen, die im Finanzsektor auftreten können, betreffen nicht nur Finanzunternehmen, die isoliert betrachtet werden. Ebenso können sich hierdurch ermittelte Schwachstellen über die Übertragungskanäle des Finanzsystems verbreiten und die Stabilität des Finanzsystems der Union beeinträchtigen, etwa durch Liquiditätsengpässe und einen allgemeinen Verlust des Vertrauens in die Finanzmärkte.

(4) Politische Entscheidungsträger, Regulierungsbehörden und Normungsgremien auf internationaler Ebene, Unionsebene und nationaler Ebene haben sich in den letzten Jahren mit dem IKT-Risiko befasst, um die digitale Resilienz zu stärken, Standards festzulegen und die Regulierungs- und Aufsichtsarbeit zu koordinieren. Auf internationaler Ebene sind der Basler Ausschuss für Bankenaufsicht, der Ausschuss für Zahlungsverkehr und Marktinfrastrukturen, der Rat für Finanzstabilität, das Institut für Finanzstabilität sowie die G7 und G20 bestrebt, den zuständigen Behörden und Marktteilnehmern in verschiedenen Rechtsordnungen Instrumente an die Hand zu geben, um die Resilienz ihrer Finanzsysteme zu stärken. Diesen Arbeiten lag auch die Notwendigkeit zugrunde, das IKT-Risiko im Kontext eines stark vernetzten globalen Finanzsystems zu berücksichtigen und sich um mehr Kohärenz der relevanten bewährten Verfahren zu bemühen.

(5) Das IKT-Risiko bleibt trotz gezielter politischer und legislativer Initiativen auf Unionsebene und nationaler Ebene eine Herausforderung für die operationale Resilienz, Leistungsfähigkeit und Stabilität des Finanzsystems der Union. Mit den Reformen nach der Finanzkrise von 2008 wurde in erster Linie die finanzielle Resilienz des Finanzsektors der Union gestärkt und darauf abgezielt, die Wettbewerbsfähigkeit und Stabilität der Union aus wirtschaftlicher, aufsichtsrechtlicher und marktpolitischer Sicht zu bewahren. Obwohl IKT-Sicherheit und digitale Resilienz Bestandteil des operationellen Risikos sind, standen sie in der Zeit nach der Finanzkrise weniger im Fokus der Regulierungsagenda und wurden nur in einigen Bereichen der Unionspolitik für Finanzdienstleistungen und Regulierung oder nur in wenigen Mitgliedstaaten weiterentwickelt.

(6) In ihrer Mitteilung mit dem Titel „FinTech-Aktionsplan: für einen wettbewerbsfähigeren und innovativen europäischen Finanzsektor“ vom 8. März 2018 hob die Kommission hervor, wie überaus wichtig es ist, den Finanzsektor der Union widerstandsfähiger zu machen, auch aus operativer Sicht, um seine technologische Sicherheit und sein reibungsloses Funktionieren sowie seine rasche Wiederherstellung nach IKT-Sicherheitsverletzungen und -Vorfällen zu gewährleisten, damit Finanzdienstleistungen in der gesamten Union — auch in Stresssituationen — wirksam und reibungslos erbracht werden können und gleichzeitig das Vertrauen der Verbraucher und der Märkte gewahrt wird.

(7) Im April 2019 veröffentlichten die mit der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates ([4]) eingerichtete Europäische Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde, EBA), die mit der Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates ([5]) eingerichtete Europäische Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung,

([4]) 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).

([5]) 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).

EIOPA) und die mit der Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates ([6]) eingerichtete Europäische Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde, ESMA) (zusammen als „Europäische Aufsichtsbehörden" oder „ESA", im Folgenden „ESA") gemeinsam fachliche Gutachten, in denen ein kohärenter Ansatz für das IKT-Risiko im Finanzbereich gefordert und empfohlen wurde, die digitale operationale Resilienz der Finanzdienstleistungsbranche durch eine sektorspezifische Initiative der Union auf verhältnismäßige Weise zu stärken.

(8) Der Finanzsektor der Union wird durch ein einheitliches Regelwerk (Single Rulebook) reguliert und unterliegt einem europäischen Finanzaufsichtssystem. Dennoch wurden Bestimmungen über die digitale operationale Resilienz und die IKT-Sicherheit noch nicht vollständig oder konsequent harmonisiert, obwohl die digitale operationale Resilienz für die Gewährleistung von Finanzstabilität und Marktintegrität im digitalen Zeitalter von entscheidender Bedeutung und nicht weniger wichtig ist als beispielsweise gemeinsame Aufsichts- oder Marktverhaltensstandards. Daher sollten das einheitliche Regelwerk und das Aufsichtssystem so weiterentwickelt werden, dass sie auch die digitale operationale Resilienz abdecken, indem die Mandate der zuständigen Behörden gestärkt werden, damit sie zur Wahrung der Integrität und der Effizienz des Binnenmarkts und zur Förderung seines ordnungsgemäßen Funktionierens des Managements des IKT-Risikos im Finanzsektor überwachen können.

(9) Rechtliche Unterschiede und ungleiche nationale Regulierungs- oder Aufsichtsansätze in Bezug auf das IKT-Risiko schaffen Hindernisse für das Funktionieren des Binnenmarkts für Finanzdienstleistungen und erschweren grenzüberschreitend tätigen Finanzunternehmen die reibungslose Ausübung der Niederlassungsfreiheit und die Erbringung von Dienstleistungen. Auch der Wettbewerb zwischen denselben Arten von Finanzunternehmen, die in verschiedenen Mitgliedstaaten tätig sind, könnte verzerrt werden. Dies gilt insbesondere in Bereichen, in denen die Harmonisierung auf Unionsebene bislang sehr begrenzt — wie beim Testen der digitalen operationalen Resilienz — oder gar nicht vorhanden ist — wie bei der Überwachung des IKT-Drittparteienrisikos. Unterschiede, die sich aus den auf nationaler Ebene geplanten Entwicklungen ergeben, könnten weitere Hindernisse für das Funktionieren des Binnenmarkts schaffen, die sich nachteilig auf die Marktteilnehmer und die Finanzstabilität auswirken.

(10) Da die einschlägigen Bestimmungen über IKT-Risiken bisher auf Unionsebene nur auf unvollständige Art und Weise angegangen wurden, bestehen Lücken oder Überschneidungen in wichtigen Bereichen — wie der Meldung IKT-bezogener Vorfälle und Tests der digitalen operationalen Resilienz — sowie Unstimmigkeiten aufgrund sich abzeichnender unterschiedlicher nationaler Vorschriften oder einer kostenineffizienten Anwendung sich überschneidender Vorschriften. Dies ist besonders schädlich für intensive IKT-Nutzer wie den Finanzsektor, da technologische Risiken keine Grenzen haben und der Finanzsektor seine Dienste auf breiter grenzüberschreitender Basis inner- und außerhalb der Union erbringt. Einzelne Finanzunternehmen, die grenzüberschreitend tätig sind oder über mehrere Zulassungen verfügen (z. B. kann ein Finanzunternehmen eine Lizenz für eine Bank, eine Wertpapierfirma und ein Zahlungsinstitut besitzen, die jeweils von einer anderen zuständigen Behörde in einem oder mehreren Mitgliedstaaten ausgestellt wurde), stehen bei der alleinigen und kohärenten und kostenwirksamen Bewältigung des IKT-Risikos und der Abmilderung nachteiliger Auswirkungen von IKT-Vorfällen vor operativen Herausforderungen.

(11) Da das einheitliche Regelwerk nicht mit einem umfassenden Rahmen für IKT oder operationelle Risiken einhergeht, ist eine weitere Harmonisierung der wichtigsten Anforderungen an die digitale operationale Resilienz für alle Finanzunternehmen erforderlich. Die Entwicklung der IKT-Kapazitäten und der allgemeinen Resilienz durch Finanzunternehmen auf der Grundlage dieser Kernanforderungen, um operativen Ausfällen standzuhalten, würde dabei helfen, die Stabilität und Integrität der Finanzmärkte der Union zu erhalten, und auf diese Weise dazu beitragen, ein hohes Schutzniveau für Anleger und Verbraucher in der Union sicherzustellen. Da diese Verordnung zum reibungslosen Funktionieren des Binnenmarkts beitragen soll, sollte sie sich auf die Bestimmungen von Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) in der Auslegung der ständigen Rechtsprechung des Gerichtshofs der Europäischen Union (im Folgenden „Gerichtshof") stützen.

(12) Mit dieser Verordnung sollen die Anforderungen mit Blick auf IKT-Risiken im Rahmen der Anforderungen an das operationelle Risiko konsolidiert und verbessert werden, die bisher in verschiedenen Rechtsakten der Union gesondert behandelt wurden. Diese Rechtsakte deckten zwar die wichtigsten Kategorien finanzieller Risiken ab (z. B. Kreditrisiko, Marktrisiko, Gegenparteiausfallrisiko, Liquiditätsrisiko und Marktrisiko), waren aber bei ihrer Annahme nicht umfassend auf alle Komponenten der operationalen Resilienz ausgerichtet. Bei der Weiterentwicklung der Vorschriften über das operationelle Risiko in diesen Rechtsakten der Union wurde häufig ein traditioneller quantitativer Ansatz zur Bewältigung von Risiken (d. h. die Festlegung einer Kapitalvorgabe zur Absicherung gegen

([6]) 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).

das IKT-Risiko) bevorzugt, anstelle gezielter qualitativer Vorschriften für den Schutz, die Erkennung, Eindämmung, Wiederherstellung und die Sanierungskapazitäten bei IKT-bezogenen Vorfällen oder für die Kapazitäten für Meldungen und Tests digitaler Technologie. Mit diesen Rechtsakten sollten in erster Linie wesentliche Vorschriften über die Beaufsichtigung, die Integrität oder das Verhalten des Marktes abgedeckt und aktualisiert werden. Indem die verschiedenen Vorschriften über IKT-Risiken konsolidiert und verbessert werden, sollten alle Bestimmungen, die sich mit digitalen Risiken im Finanzsektor befassen, erstmals in einheitlicher Weise in einem einzigen Rechtsakt zusammengefasst werden. Somit schließt diese Verordnung Lücken oder behebt Unstimmigkeiten in einigen der vorausgehenden Rechtsakte (auch in Bezug auf die darin verwendete Terminologie) und nimmt durch gezielte Vorschriften über die Kapazitäten für das IKT-Risikomanagement, die Meldung von Vorfällen, Tests der operationalen Resilienz sowie die Überwachung des IKT-Drittparteienrisikos ausdrücklich auf IKT-Risiken Bezug. Somit sollte diese Verordnung auch für das IKT-Risiko sensibilisieren und berücksichtigen, dass die finanzielle Solidität von Finanzunternehmen durch IKT-Vorfälle und eine mangelnde operationale Resilienz beeinträchtigt werden könnten.

(13) Finanzunternehmen sollten bei der Bewältigung von IKT-Risiken denselben Ansatz und dieselben grundsatzbasierten Regeln befolgen, wobei ihrer Größe und ihrem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte Rechnung zu tragen ist. Kohärenz trägt dazu bei, das Vertrauen in das Finanzsystem zu stärken und dessen Stabilität zu erhalten, insbesondere in Zeiten starker Abhängigkeit von IKT-Systemen, -Plattformen und -Infrastrukturen, die erhöhtes digitales Risiko mit sich bringt. Ebenso sollte durch Einhaltung einer grundlegenden Cyberhygiene verhindert werden, dass der Wirtschaft durch die Minimierung der Auswirkungen und Kosten von IKT-Störfällen hohe Kosten entstehen.

(14) Eine Verordnung hilft, die Komplexität der Regulierung zu verringern, fördert die aufsichtliche Konvergenz, erhöht die Rechtssicherheit und trägt ferner dazu bei, die Befolgungskosten, insbesondere für grenzüberschreitend tätige Finanzunternehmen, zu begrenzen und Wettbewerbsverzerrungen zu verringern. Daher ist die Wahl einer Verordnung zur Schaffung eines gemeinsamen Rahmens für die digitale operationale Resilienz von Finanzunternehmen am besten geeignet, eine einheitliche und kohärente Anwendung aller Komponenten des IKT-Risikomanagements im Finanzsektor der Union zu gewährleisten.

(15) Die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([7]) stellte den ersten horizontalen Rahmen für die Cybersicherheit auf Unionsebene dar, der auch für drei Arten von Finanzunternehmen, namentlich für Kreditinstitute, Handelsplätze und zentrale Gegenparteien gilt. Da in der Richtlinie (EU) 2016/1148 jedoch ein Mechanismus zur Identifizierung der Betreiber wesentlicher Dienste auf nationaler Ebene vorgesehen ist, wurden nur bestimmte Kreditinstitute, Handelsplätze und zentrale Gegenparteien, die von den Mitgliedstaaten ermittelt wurden, in der Praxis in den Anwendungsbereich der Richtlinie aufgenommen und daher verpflichtet, die darin festgelegten Anforderungen an die IKT-Sicherheit und die Meldung von Vorfällen zu erfüllen. Die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates ([8]) legt ein einheitliches Kriterium dafür fest, welche Unternehmen in ihren Anwendungsbereich fallen (Schwellenwert für die Größe), wobei auch die drei Arten von Finanzunternehmen in ihrem Anwendungsbereich verbleiben.

(16) Da mit dieser Verordnung jedoch das Ausmaß der Harmonisierung in Bezug auf die verschiedenen Komponenten der digitalen Resilienz erhöht wird, indem Anforderungen an das IKT-Risikomanagement und die Meldung von IKT-Vorfällen eingeführt werden, die strenger sind als diejenigen im aktuellen Finanzdienstleistungsrecht der Union, stellt dies auch im Vergleich zu den Anforderungen der Richtlinie (EU) 2022/2555 eine stärkere Harmonisierung dar. Folglich verkörpert diese Verordnung eine *Lex specialis* zur Richtlinie (EU) 2022/2555. Es ist zugleich von entscheidender Bedeutung, dass eine enge Beziehung zwischen dem Finanzsektor und dem derzeit in der Richtlinie (EU) 2022/2555 festgelegten horizontalen Rahmen der Union für Cybersicherheit aufrechterhalten wird, um die Kohärenz mit den von den Mitgliedstaaten angenommenen Strategien für Cybersicherheit zu gewährleisten und es Finanzaufsichtsbehörden zu ermöglichen, auf Cybervorfälle aufmerksam gemacht zu werden, die andere unter die genannte Richtlinie fallende Sektoren betreffen.

([7]) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

([8]) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (siehe Seite 80 dieses Amtsblatts).

(17) Im Einklang mit Artikel 4 Absatz 2 des Vertrags über die Europäische Union und unbeschadet der gerichtlichen Überprüfung durch den Gerichtshof sollte diese Verordnung die Zuständigkeit der Mitgliedstaaten für die grundlegenden Funktionen des Staates in Bezug auf die öffentliche Sicherheit, die Verteidigung und den Schutz der nationalen Sicherheit — z. B. in Bezug auf die Bereitstellung von Informationen, die dem Schutz der nationalen Sicherheit zuwiderlaufen würden — unberührt lassen.

(18) Um sektorübergreifendes Lernen zu ermöglichen und Erfahrungen anderer Sektoren beim Umgang mit Cyberbedrohungen wirksam zu nutzen, sollten Finanzunternehmen im Sinne der Richtlinie (EU) 2022/2555 Teil des „Ökosystems" jener Richtlinie bleiben (z. B. Kooperationsgruppe und Computer-Notfallteam (computer security incident response team, CSIRT)). Die ESA und zuständige nationale Behörden sollten in der Lage sein, sich an den strategischen politischen Diskussionen und der technischen Arbeit der Kooperationsgruppe im Sinne der genannten Richtlinie zu beteiligen, Informationen austauschen und mit den entsprechend der genannten Richtlinie benannten oder eingerichteten zentralen Anlaufstellen weiter zusammenarbeiten. Die nach der vorliegenden Verordnung zuständigen Behörden sollten auch die CSIRT konsultieren und mit ihnen zusammenarbeiten. Darüber hinaus sollten die zuständigen Behörden die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden um fachliche Beratung ersuchen und Kooperationsvereinbarungen schließen können, mit denen wirksame und schnelle Koordinierungsmechanismen sichergestellt werden sollen.

(19) Angesichts der engen Verflechtungen zwischen der digitalen Resilienz und der physischen Resilienz von Finanzunternehmen ist in der vorliegenden Verordnung und in der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates ([9]) ein kohärenter Ansatz in Bezug auf die Resilienz kritischer Einrichtungen erforderlich. Da das IKT-Risikomanagement und die Meldepflichten nach der vorliegenden Verordnung der physischen Resilienz von Finanzunternehmen umfassend Rechnung tragen, sollten die in den Kapiteln III und IV der Richtlinie (EU) 2022/2557 festgelegten Verpflichtungen nicht für Finanzunternehmen gelten, die in den Anwendungsbereich der genannten Richtlinie fallen.

(20) Anbieter von Cloud-Computing-Diensten sind eine Kategorie digitaler Infrastruktur, die unter die Richtlinie (EU) 2022/2555 fällt. Der mit dieser Verordnung geschaffene Überwachungsrahmen der Union (im Folgenden „Überwachungsrahmen") gilt für alle kritischen IKT-Drittdienstleister, einschließlich Anbietern von Cloud-Computing-Diensten, die Finanzunternehmen IKT-Dienstleistungen bereitstellen, und sollte als Ergänzung zu der Beaufsichtigung gemäß der Richtlinie (EU) 2022/2555 betrachtet werden. Darüber hinaus sollte der mit dieser Verordnung geschaffene Überwachungsrahmen für Anbieter von Cloud-Computing-Diensten gelten, wenn es keinen horizontalen Rahmen der Union gibt, mit dem eine Behörde für die digitale Überwachung eingerichtet wird.

(21) Um die vollständige Kontrolle über das IKT-Risiko zu behalten, müssen Finanzunternehmen über umfassende Kapazitäten verfügen, die ein leistungsfähiges und wirksames IKT-Risikomanagement sowie spezifische Mechanismen und Strategien für die Handhabung aller IKT-bezogener Vorfälle und für die Meldung schwerwiegender IKT-bezogener Vorfälle ermöglichen. Ebenso sollten Finanzunternehmen über Leit- und Richtlinien für die Erprobung von IKT-Systemen, -Kontrollen und -Prozessen sowie für das Management des IKT-Drittparteienrisikos verfügen. Die Mindestanforderungen an die digitale operationale Resilienz für Finanzunternehmen sollten angehoben werden, wobei auch eine verhältnismäßige Anwendung der Anforderungen für bestimmte Finanzunternehmen möglich sein sollte, insbesondere bei Kleinstunternehmen sowie Finanzunternehmen, die einem vereinfachten IKT-Risikomanagementrahmen unterliegen. Um eine effiziente Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung zu ermöglichen, die verhältnismäßig ist und der Notwendigkeit Rechnung trägt, den Verwaltungsaufwand für die zuständigen Behörden zu verringern, sollten die einschlägigen nationalen Aufsichtsmechanismen für derartige Finanzunternehmen deren Größe und Gesamtrisikoprofil sowie die Art, den Umfang und die Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte berücksichtigen, auch wenn die in Artikel 5 der Richtlinie (EU) 2016/2341 des Europäischen Parlaments und des Rates ([10]) festgelegten einschlägigen Schwellenwerte überschritten werden. Insbesondere sollten sich die Aufsichtstätigkeiten vorrangig auf die Notwendigkeit konzentrieren, ernsthaften Risiken im Zusammenhang mit dem IKT-Risikomanagement eines bestimmten Unternehmens entgegenzuwirken.

([9]) Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (siehe Seite 164 dieses Amtsblatts).

([10]) Richtlinie (EU) 2016/2341 des Europäischen Parlaments und des Rates vom 14. Dezember 2016 über die Tätigkeiten und die Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung (EbAV) (ABl. L 354 vom 23.12.2016, S. 37).

Die zuständigen Behörden sollten auch einen wachsamen, aber verhältnismäßigen Ansatz in Bezug auf die Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung verfolgen, die gemäß Artikel 31 der Richtlinie (EU) 2016/2341 einen wesentlichen Teil ihres Kerngeschäfts, wie Vermögensverwaltung, versicherungsmathematische Berechnungen, Rechnungslegung und Datenverwaltung, an Dienstleister auslagern.

(22) Die Schwellenwerte und Taxonomien für die Meldung IKT-bezogener Vorfälle unterscheiden sich auf nationaler Ebene erheblich. Wenngleich sich durch einschlägige Arbeiten der durch die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates ([11]) eingerichtete Agentur der Europäischen Union für Cybersicherheit (ENISA) und der Kooperationsgruppe im Sinne der Richtlinie (EU) 2022/2555 eine gemeinsame Grundlage schaffen lässt, bestehen für die übrigen Finanzunternehmen noch immer unterschiedliche Ansätze in Bezug auf die Festlegung der Schwellenwerte und die Verwendung von Taxonomien bzw. können sich für diese ergeben. Aufgrund dieser Unterschiede besteht eine Vielzahl von Anforderungen, die Finanzunternehmen einhalten müssen, insbesondere wenn sie in mehreren Mitgliedstaaten tätig sind und Teil einer Finanzgruppe sind. Darüber hinaus können derartige Unterschiede die Einrichtung weiterer einheitlicher oder zentralisierter Mechanismen der Union behindern, die das Meldeverfahren beschleunigen und einen raschen und reibungslosen Informationsaustausch zwischen den zuständigen Behörden unterstützen, was für die Bewältigung des IKT-Risikos bei Großangriffen mit potenziell systemischen Folgen von entscheidender Bedeutung ist.

(23) Um für bestimmte Finanzunternehmen den Verwaltungsaufwand zu verringern und potenziell doppelte Meldepflichten zu vermeiden, sollte die Verpflichtung zur Meldung von Vorfällen gemäß der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates ([12]) nicht mehr für Zahlungsdienstleister gelten, die in den Geltungsbereich dieser Verordnung fallen. Folglich sollten Kreditinstitute, E-Geld-Institute, Zahlungsinstitute und Kontoinformationsdienstleister im Sinne von Artikel 33 Absatz 1 der genannten Richtlinie alle zahlungsbezogenen Betriebs- oder Sicherheitsvorfälle, die vormals gemäß der genannten Richtlinie gemeldet wurden, ab dem Geltungsbeginn dieser Verordnung gemäß dieser melden, und zwar unabhängig davon, ob es sich um IKT-bezogene Vorfälle handelt oder nicht.

(24) Um den zuständigen Behörden die Erfüllung von Aufsichtsaufgaben zu ermöglichen, indem sie einen vollständigen Überblick über Art, Häufigkeit, Ausmaß und Auswirkungen IKT-bezogener Vorfälle erhalten, und um den Informationsaustausch zwischen einschlägigen Behörden, einschließlich Strafverfolgungs- und Abwicklungsbehörden, zu verbessern, sollte diese Verordnung eine solide Regelung für die Meldung IKT-bezogener Vorfälle festlegen, wobei die einschlägigen Anforderungen derzeitige Lücken im Finanzdienstleistungsrecht schließen, und Überschneidungen und Doppelarbeit mit Blick auf eine Senkung der Kosten beseitigen. Es ist von entscheidender Bedeutung, die Regelung für die Meldung IKT-bezogener Vorfälle zu harmonisieren, indem alle Finanzunternehmen verpflichtet werden, ihren zuständigen Behörden in dem in dieser Verordnung vorgesehenen einheitlichen, gestrafften Rahmen Bericht zu erstatten. Darüber hinaus sollten die ESA ermächtigt werden, relevante Aspekte für den Rahmen für die Meldung IKT-bezogener Vorfälle — wie Taxonomie, Zeitrahmen, Datensätze, Vorlagen und anwendbare Schwellenwerte — näher zu spezifizieren. Um vollständige Übereinstimmung mit der Richtlinie (EU) 2022/2555 zu gewährleisten, sollten Finanzunternehmen der jeweils zuständigen Behörde auf freiwilliger Basis erhebliche Cyberbedrohungen melden können, wenn sie der Auffassung sind, dass die Cyberbedrohung für das Finanzsystem, die Dienstnutzer oder die Kunden relevant ist.

(25) In einigen Teilsektoren des Finanzsektors wurden Anforderungen für Tests der digitalen operationalen Resilienz entwickelt, deren Rahmen nicht immer vollständig aneinander angeglichen waren. Dies führt zu potenziell doppelten Kosten für grenzüberschreitend tätige Finanzunternehmen und verkompliziert die gegenseitige Anerkennung der Ergebnisse von Tests der digitalen operationalen Resilienz, was wiederum zu einer Fragmentierung des Binnenmarkts führen könnte.

([11]) Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

([12]) Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35).

(26) Darüber hinaus bleiben Schwachstellen, wenn keine IKT-Tests vorgeschrieben sind, unentdeckt, wodurch ein Finanzunternehmen IKT-Risiken ausgesetzt wird und letztlich ein höheres Risiko für die Stabilität und Integrität des Finanzsektors entsteht. Ohne ein Tätigwerden der Union wären Tests der digitalen operationalen Resilienz weiterhin uneinheitlich, und es gäbe kein System für die gegenseitige Anerkennung der IKT-Testergebnisse in verschiedenen Rechtsordnungen. Da es unwahrscheinlich ist, dass Testregelungen in anderen Teilsektoren des Finanzsektors in bedeutendem Umfang eingeführt würden, gingen darüber hinaus die potenziellen Vorteile eines Rahmens für Tests im Hinblick auf die Aufdeckung von Schwachstellen und Risiken sowie von Tests von Verteidigungsfähigkeiten und die Fortführung der Geschäftstätigkeit verloren, die zur Stärkung des Vertrauens von Kunden, Lieferanten und Geschäftspartnern beitragen. Um diese Überschneidungen, Divergenzen und Lücken zu beseitigen, müssen Vorschriften für ein koordiniertes Testsystem festgelegt werden, damit die gegenseitige Anerkennung erweiterter Tests für diejenigen Finanzunternehmen erleichtert wird, die die Kriterien in dieser Verordnung erfüllen.

(27) Die Abhängigkeit der Finanzunternehmen von IKT-Dienstleistungen ist zum Teil darauf zurückzuführen, dass sie sich an eine sich entwickelnde wettbewerbsorientierte digitale Weltwirtschaft anpassen, ihre geschäftliche Effizienz steigern und die Verbrauchernachfrage befriedigen müssen. Die Art und das Ausmaß dieser Nutzung von IKT-Dienstleistungen haben sich in den letzten Jahren ständig weiterentwickelt, was zu Kostensenkungen bei der Finanzintermediation geführt hat, die Expansion von Unternehmen und die Skalierbarkeit bei der Ausübung von Finanztätigkeiten ermöglicht und gleichzeitig ein breites Spektrum an IKT-Tools für die Verwaltung komplexer interner Prozesse zur Verfügung gestellt hat.

(28) Die umfangreiche Nutzung von IKT-Dienstleistungen zeigt sich an komplexen vertraglichen Vereinbarungen, wobei Finanzunternehmen häufig Schwierigkeiten haben, Vertragsbedingungen auszuhandeln, die auf die Aufsichtsstandards oder sonstige aufsichtsrechtliche Anforderungen, denen sie unterliegen, zugeschnitten sind; Gleiches gilt für die Durchsetzung bestimmter Rechte, wie Zugangs- oder Auditrechte, selbst wenn diese in ihren vertraglichen Vereinbarungen verankert sind. Darüber hinaus fehlen in vielen dieser vertraglichen Vereinbarungen ausreichende Garantien, die die vollständige Überwachung von Verfahren für die Unterauftragsvergabe ermöglichen, wodurch das Finanzunternehmen die damit verbundenen Risiken nicht bewerten kann. Da IKT-Drittdienstleister häufig standardisierte Dienstleistungen für verschiedene Arten von Kunden anbieten, wird den individuellen oder spezifischen Bedürfnissen der Akteure der Finanzbranche in derartigen vertraglichen Vereinbarungen nicht immer angemessen Rechnung getragen.

(29) Obwohl die Rechtsvorschriften für Finanzdienstleistungen bestimmte allgemeine Vorschriften über die Auslagerung von Tätigkeiten enthalten, ist die Überwachung der vertraglichen Dimension nicht vollständig in den Rechtsvorschriften der Union verankert. Weil eindeutige und angepasste Unionsstandards, die auf die vertraglichen Vereinbarungen mit IKT-Drittdienstleistern anwendbar sind, fehlen, werden externe Quellen für IKT-Risiken nicht umfassend behandelt. Daher müssen bestimmte Schlüsselprinzipien festgelegt werden, die Finanzunternehmen als Richtschnur für das Management des IKT-Drittparteienrisikos dienen und von besonderer Bedeutung sind, wenn Finanzunternehmen zur Unterstützung ihrer kritischen oder wichtigen Funktionen auf IKT-Drittdienstleister zurückgreifen. Diese Prinzipien sollten mit einer Reihe grundlegender vertraglicher Rechte einhergehen, die sich auf mehrere Aspekte bei der Erfüllung und Beendigung von vertraglichen Vereinbarungen beziehen, damit bestimmte Mindestgarantien geboten werden, um die Fähigkeit von Finanzunternehmen, alle von Drittdienstleistern ausgehenden IKT-Risiken wirksam zu überwachen, zu stärken. Diese Prinzipien ergänzen die für die Auslagerung geltenden sektorspezifischen Rechtsvorschriften.

(30) Ein gewisser Mangel an Homogenität und Konvergenz in Bezug auf die Überwachung des IKT-Drittparteienrisikos und die Abhängigkeit von IKT-Drittdienstleistern ist derzeit festzustellen. Obwohl Anstrengungen unternommen wurden, um den Bereich der Auslagerung anzugehen, wie beispielsweise die Leitlinien der EBA zu Auslagerung von 2019 und Leitlinien der ESMA zur Auslagerung an Cloud-Anbieter von 2021, wird die allgemeinere Frage der Eindämmung systemischer Risiken, die entstehen könnten, wenn der Finanzsektor einer begrenzten Anzahl kritischer IKT-Drittdienstleister ausgesetzt ist, im Unionsrecht nicht ausreichend behandelt. Der Mangel an Vorschriften auf Unionsebene wird noch dadurch verschärft, dass es keine nationalen Vorschriften für die Mandate und Instrumente gibt, die es Finanzaufsichtsbehörden ermöglichen, Abhängigkeiten von IKT-Drittdienstleistern ordnungsgemäß zu erfassen und Risiken, die sich aus der Konzentration der Abhängigkeiten von IKT-Drittdienstleistern ergeben, angemessen zu überwachen.

(31) Unter Berücksichtigung der potenziellen Systemrisiken, die mit der verstärkten Auslagerung und der Konzentration der Abhängigkeiten von IKT-Drittdienstleistern verbunden sind, und in Anbetracht nationaler Regelungen, die den Finanzaufsichtsbehörden unzureichend Werkzeuge bereitstellen, die geeignet sind, die Folgen der bei kritischen IKT-Drittdienstleistern auftretenden IKT-Risiken zu quantifizieren, zu qualifizieren und zu beheben, muss ein geeigneter Überwachungsrahmen geschaffen werden, der eine kontinuierliche Überwachung der Tätigkeiten von IKT-Drittdienstleistern, bei denen es sich um für Finanzunternehmen kritische IKT-Drittdienstleister handelt, ermöglicht und zugleich bei Kunden, bei denen es sich nicht um Finanzunternehmen handelt, Vertraulichkeit und Sicherheit gewährleistet. Auch wenn mit der gruppeninternen Bereitstellung von IKT-Dienstleistungen spezifische Risiken und Vorteile einhergehen, sollte sie nicht automatisch als weniger riskant angesehen werden als die Bereitstellung von IKT-Dienstleistungen durch Dienstleister außerhalb einer Finanzgruppe und sollte daher demselben Rechtsrahmen unterliegen. Wenn IKT-Dienstleistungen innerhalb einer Finanzgruppe bereitgestellt werden, könnten Finanzunternehmen möglicherweise jedoch ein höheres Maß an Kontrolle über gruppeninterne Dienstleister haben, was bei der Gesamtrisikobewertung berücksichtigt werden sollte.

(32) Da IKT- Risiken immer komplexer und technisch ausgereifter werden, hängen gute Maßnahmen für die Erkennung und Prävention von IKT-Risiken in hohem Maße von einem regelmäßigen Informationsaustausch zwischen Finanzunternehmen über Bedrohungen und Schwachstellen ab. Ein Informationsaustausch trägt dazu bei, das Bewusstsein für Cyberbedrohungen zu schärfen. Dies wiederum verstärkt die Fähigkeit der Finanzunternehmen, zu verhindern, dass Cyberbedrohungen in reale IKT-bezogene Vorfälle münden, und versetzt Finanzunternehmen in die Lage, die Auswirkungen IKT-bezogener Vorfälle wirksamer einzudämmen und sich schneller zu erholen. In Ermangelung von Leitlinien auf Unionsebene scheinen mehrere Faktoren einen solchen Wissensaustausch verhindert zu haben, darunter insbesondere die Unsicherheit hinsichtlich der Vereinbarkeit mit den Datenschutz-, Kartell- und Haftungsvorschriften.

(33) Darüber hinaus führen Zweifel bezüglich der Art von Informationen, die mit anderen Marktteilnehmern oder mit Nicht-Aufsichtsbehörden (z. B. ENISA für analytische Eingaben oder Europol für Strafverfolgungszwecke) ausgetauscht werden können, dazu, dass nützliche Informationen vorenthalten werden. Deswegen sind Umfang und Qualität des Informationsaustauschs derzeit nach wie vor begrenzt und fragmentiert, wobei der einschlägige Austausch hauptsächlich auf lokaler Ebene (über nationale Initiativen) erfolgt und keine einheitlichen unionsweiten Regelungen für den Informationsaustausch bestehen, die auf die Bedürfnisse eines integrierten Finanzsystems zugeschnitten sind. Aus diesem Grund ist es wichtig, diese Kommunikationskanäle zu stärken.

(34) Finanzunternehmen sollten ermutigt werden, Informationen und Erkenntnisse zu Cyberbedrohungen untereinander auszutauschen und ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam zu nutzen, damit sich ihre Fähigkeit verbessert, Cyberbedrohungen angemessen zu bewerten, zu überwachen, abzuwehren und auf sie zu reagieren, indem sie an Vereinbarungen über den Austausch von Informationen teilnehmen. Daher muss auf Unionsebene die Einrichtung von Regelungen für freiwillige Vereinbarungen über den Informationsaustausch ermöglicht werden, die — bei der Umsetzung in vertrauenswürdigen Umgebungen — der Finanzwelt dabei helfen würden, Cyberbedrohungen vorzubeugen und gemeinsam auf diese zu reagieren, indem die Ausbreitung von IKT-Risiken rasch eingedämmt und potenzielle Ansteckungseffekte über alle Finanzkanäle hinweg verhindert werden. Diese Regelungen sollten mit dem anwendbaren Wettbewerbsrecht der Union, das in der Mitteilung der Kommission vom 14. Januar 2011 mit dem Titel „Leitlinien zur Anwendbarkeit des Artikels 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über horizontale Zusammenarbeit“ sowie den Datenschutzvorschriften der Union und insbesondere der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([13]) im Einklang stehen. Sie sollten auf der Grundlage einer oder mehrerer der in Artikel 6 jener Verordnung festgelegten Rechtsgrundlagen tätig werden, beispielsweise im Zusammenhang mit der Verarbeitung personenbezogener Daten, die zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten gemäß Artikel 6 Absatz 1 Buchstabe f jener Verordnung erforderlich ist, sowie im Zusammenhang mit der Verarbeitung personenbezogener Daten, die für die Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, gemäß Artikel 6 Absatz 1 Buchstabe c bzw. e jener Verordnung erforderlich ist.

([13]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), (ABl. L 119 vom 4.5.2016, S. 1).

(35) Um ein hohes Niveau an digitaler operationaler Resilienz im gesamten Finanzsektor aufrechtzuerhalten und zugleich mit den technologischen Entwicklungen Schritt zu halten, sollte in der vorliegenden Verordnung auf Risiken eingegangen werden, die sich aus allen Arten von IKT-Dienstleistungen ergeben. Zu diesem Zweck sollte die Definition von IKT-Dienstleistungen im Zusammenhang mit der vorliegenden Verordnung weit ausgelegt werden und digitale Dienste und Datendienste umfassen, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern fortlaufend bereitgestellt werden. Diese Definition sollte beispielsweise sogenannte „Over-the-top"-Dienste umfassen, die unter die Kategorie der elektronischen Kommunikationsdienste fallen. Sie sollte nur die begrenzte Kategorie traditioneller analoger Telefondienste ausschließen, die als Dienste des öffentlichen Fernsprechnetzes (PSTN — Public Switched Telephone Network), Festnetz-Dienste, herkömmliche Fernsprechdienste (POTS — Plain Old Telephone Service) oder Festnetztelefondienste gelten.

(36) Ungeachtet des in dieser Verordnung vorgesehenen breiten Geltungsbereichs sollten bei der Anwendung der Vorschriften für die digitale operationale Resilienz die wesentlichen Unterschiede zwischen Finanzunternehmen in Bezug auf deren Größe und Gesamtrisikoprofil berücksichtigt werden. Als Grundprinzip sollten Finanzunternehmen bei der Verteilung von Ressourcen und Kapazitäten für die Umsetzung des Rahmens für das IKT-Risikomanagement ihren IKT-Bedarf sorgfältig auf ihre Größe und ihr Gesamtrisikoprofil sowie die Art, den Umfang und die Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte abstimmen, während die zuständigen Behörden den Ansatz einer solchen Verteilung weiterhin bewerten und überprüfen sollten.

(37) Die in Artikel 33 Absatz 1 der Richtlinie (EU) 2015/2366 genannten Kontoinformationsdienstleister werden unter Berücksichtigung der Besonderheiten ihrer Tätigkeiten und der mit ihnen verbundenen Risiken ausdrücklich in den Geltungsbereich der vorliegenden Verordnung einbezogen. Darüber hinaus fallen gemäß Artikel 9 Absatz 1 der Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates ([14]) und Artikel 32 Absatz 1 der Richtlinie (EU) 2015/2366 ausgenommene E-Geld-Institute und Zahlungsinstitute auch dann in den Geltungsbereich dieser Verordnung, wenn ihnen keine Zulassung gemäß der Richtlinie 2009/110/EG für die Ausgabe von E-Geld erteilt wurde oder wenn ihnen keine Zulassung für die Erbringung und Ausführung von Zahlungsdiensten gemäß der Richtlinie (EU) 2015/2366 erteilt wurde. Postscheckämter im Sinne von Artikel 2 Absatz 5 Nummer 3 der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates ([15]) sind jedoch vom Geltungsbereich der vorliegenden Verordnung ausgenommen. Die zuständige Behörde für die nach der Richtlinie (EU) 2015/2366 ausgenommenen Zahlungsinstitute, die nach der Richtlinie 2009/110/EG ausgenommenen E-Geld-Institute und die Kontoinformationsdienstleister im Sinne von Artikel 33 Absatz 1 der Richtlinie (EU) 2015/2366 sollte die gemäß Artikel 22 der Richtlinie (EU) 2015/2366 benannte zuständige Behörde sein.

(38) Da größere Finanzunternehmen unter Umständen über umfangreichere Ressourcen verfügen und rasch Mittel für die Einrichtung von Governance-Strukturen und die Einführung verschiedener Unternehmensstrategien bereitstellen könnten, sollten nur Finanzunternehmen, die keine Kleinstunternehmen im Sinne dieser Verordnung sind, verpflichtet werden, komplexere Governance-Regelungen einzuführen. Diese Unternehmen sind besser gerüstet, um insbesondere spezielle Managementfunktionen für die Überwachung von Vereinbarungen mit IKT-Drittdienstleistern oder für den Umgang mit dem Krisenmanagement einzurichten, ihr IKT-Risikomanagement nach dem Modell der drei Verteidigungslinien zu strukturieren oder ein internes Modell für Risikomanagement und Kontrolle einzuführen und ihren IKT-Risikomanagementrahmen internen Revisionen zu unterziehen.

(39) Einige Finanzunternehmen kommen in den Genuss von Ausnahmen oder unterliegen gemäß dem einschlägigen sektorspezifischen Unionsrecht einem sehr lockeren Regelungsrahmen. Zu diesen Finanzunternehmen zählen Verwalter alternativer Investmentfonds im Sinne von Artikel 3 Absatz 2 der Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates ([16]), Versicherungs- und Rückversicherungsunternehmen im Sinne von Artikel 4 der Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates ([17]) und Einrichtungen der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt nicht mehr als 15 Versorgungs-

([14]) Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG (ABl. L 267 vom 10.10.2009, S. 7).

([15]) Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

([16]) Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates vom 8. Juni 2011 über die Verwalter alternativer Investmentfonds und zur Änderung der Richtlinien 2003/41/EG und 2009/65/EG und der Verordnungen (EG) Nr. 1060/2009 und (EU) Nr. 1095/2010 (ABl. L 174 vom 1.7.2011, S. 1).

([17]) Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) (ABl. L 335 vom 17.12.2009, S. 1).

anwärtern betreiben. Angesichts dieser Ausnahmen wäre es nicht verhältnismäßig, diese Finanzunternehmen in den Geltungsbereich der vorliegenden Verordnung aufzunehmen. Darüber hinaus wird in der vorliegenden Verordnung den strukturellen Besonderheiten des Versicherungsvermittlermarkts Rechnung getragen, sodass Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, die als Kleinstunternehmen oder als kleine oder mittlere Unternehmen gelten, nicht unter diese Verordnung fallen sollten.

(40) Da die in Artikel 2 Absatz 5 Nummern 4 bis 23 der Richtlinie 2013/36/EU genannten Einrichtungen vom Anwendungsbereich jener Richtlinie ausgenommen sind, sollten die Mitgliedstaaten beschließen können, diejenigen dieser Einrichtungen, die sich in ihrem jeweiligen Hoheitsgebiet befinden, von der Anwendung dieser Verordnung auszunehmen.

(41) Um diese Verordnung an den Anwendungsbereich der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates ([18]) anzugleichen, ist es auch angezeigt, diejenigen in Artikel 2 und 3 jener Richtlinie genannten natürlichen und juristischen Personen, die Wertpapierdienstleistungen erbringen dürfen, ohne eine Zulassung gemäß der genannten Richtlinie erhalten zu müssen, vom Geltungsbereich der vorliegenden Verordnung auszunehmen. Nach Artikel 2 der Richtlinie 2014/65/EU sind jedoch auch Unternehmen, die für die Zwecke der vorliegenden Verordnung als Finanzunternehmen gelten, wie Zentralverwahrer, Organismen für gemeinsame Anlagen oder Versicherungs- und Rückversicherungsunternehmen, vom Anwendungsbereich der genannten Richtlinie ausgenommen. Die Ausnahme der in den Artikeln 2 und 3 jener Richtlinie genannten Personen und Unternehmen vom Geltungsbereich der vorliegenden Verordnung sollte nicht für diese Zentralverwahrer, Organismen für gemeinsame Anlagen oder Versicherungs- und Rückversicherungsunternehmen gelten.

(42) Nach dem sektorspezifischen Unionsrecht unterliegen einige Finanzunternehmen aufgrund ihrer Größe oder den von ihnen erbrachten Dienstleistungen weniger strengen Anforderungen oder Ausnahmen. Diese Kategorie von Finanzunternehmen umfasst auch kleine und nicht verflochtene Wertpapierfirmen, kleine Einrichtungen der betrieblichen Altersversorgung, die unter den in Artikel 5 der Richtlinie (EU) 2016/2341 festgelegten Bedingungen durch die betroffenen Mitgliedstaaten vom Anwendungsbereich jener Richtlinie ausgenommen werden können und Altersversorgungssysteme betreiben, die zusammen nicht mehr als 100 Mitglieder haben, sowie gemäß der Richtlinie 2013/36/EU ausgenommene Institute. Im Einklang mit dem Grundsatz der Verhältnismäßigkeit und zur Wahrung des Geistes des sektorspezifischen Unionsrechts ist es daher auch angezeigt, diese Finanzunternehmen durch die vorliegende Verordnung einem vereinfachten IKT-Risikomanagementrahmen zu unterwerfen. Die Verhältnismäßigkeit des IKT-Risikomanagementrahmens für diese Finanzunternehmen sollte durch die von den ESA zu entwickelnden technischen Regulierungsstandards nicht verändert werden. Darüber hinaus ist es im Einklang mit dem Grundsatz der Verhältnismäßigkeit angezeigt, durch die vorliegende Verordnung auch Zahlungsinstitute im Sinne des Artikels 32 Absatz 1 der Richtlinie (EU) 2015/2366 und E-Geld-Institute im Sinne des Artikels 9 der Richtlinie 2009/110/EG, die gemäß dem nationalen Recht, das diese Rechtsakte der Union umsetzt, ausgenommen sind, einem vereinfachten IKT-Risikomanagementrahmen zu unterwerfen, während Zahlungsinstitute und E-Geld-Institute, die gemäß der jeweiligen Umsetzung des sektorspezifischen Unionsrechts nicht ausgenommen wurden, den in der vorliegenden Verordnung festgelegten allgemeinen Rahmen einhalten sollten.

(43) Ebenso sollten Finanzunternehmen, die als Kleinstunternehmen gelten oder dem vereinfachten IKT-Risikomanagementrahmen nach dieser Verordnung unterliegen, nicht verpflichtet sein, eine Funktion zur Überwachung ihrer mit IKT-Drittdienstleistern geschlossenen Vereinbarungen über die Nutzung von IKT-Dienstleistungen einzurichten oder ein Mitglied der Geschäftsleitung zu benennen, das für die Überwachung der damit verbundenen Risikoexposition und die einschlägige Dokumentation zuständig ist, die Verantwortung für das Management und die Überwachung von IKT-Risiken einer Kontrollfunktion zuzuweisen und zur Vermeidung von Interessenkonflikten ein angemessenes Maß an Unabhängigkeit dieser Kontrollfunktion sicherzustellen, den IKT-Risikomanagementrahmen mindestens einmal jährlich zu dokumentieren und zu überprüfen, den IKT-Risikomanagementrahmen regelmäßig einer internen Revision zu unterziehen, nach größeren Veränderungen ihrer Netzwerk- und Informationssysteminfrastrukturen und -prozesse eingehende Bewertungen durchzuführen, regelmäßig Risikoanalysen von IKT-Altsystemen vorzunehmen, die Umsetzung der IKT-Reaktions- und Wiederherstellungspläne einer unabhängigen internen Revision zu unterziehen, eine Krisenmanagementfunktion festzulegen, die Tests der Geschäftsfortführungspläne und der Reaktions- und Wiederherstellungspläne zur Erfassung von Szenarien für die Umstellung von primärer IKT-Infrastruktur auf redundante Systeme auszuweiten, den zuständigen Behörden auf deren Anfrage eine

([18]) Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349).

Schätzung der von schwerwiegenden IKT-bezogenen Vorfällen verursachten aggregierten jährlichen Kosten und Verluste vorzulegen, redundante IKT-Kapazitäten zu unterhalten, den zuständigen nationalen Behörden die nach nachträglichen Prüfungen IKT-bezogener Vorfälle vorgenommenen Änderungen zu melden, die einschlägigen technologischen Entwicklungen fortlaufend zu überwachen, als integralen Bestandteil des in dieser Verordnung vorgesehenen IKT-Risikomanagementrahmens ein umfassendes Programm für Tests der digitalen operationalen Resilienz einzurichten oder eine Strategie für das IKT-Drittparteienrisiko zu verabschieden und regelmäßig zu überprüfen. Darüber hinaus sollten Kleinstunternehmen nur verpflichtet sein, auf der Grundlage ihres Risikoprofils zu bewerten, ob diese redundanten IKT-Kapazitäten unterhalten werden müssen. Kleinstunternehmen sollten in den Genuss einer flexibleren Regelung für Programme für Tests der digitalen operationalen Resilienz kommen. Bei der Erwägung der Art und Häufigkeit der durchzuführenden Tests sollten sie ein angemessenes Gleichgewicht zwischen dem Ziel der Aufrechterhaltung einer hohen digitalen operationalen Resilienz, den verfügbaren Ressourcen und ihrem Gesamtrisikoprofil finden. Kleinstunternehmen und Finanzunternehmen, die dem vereinfachten IKT-Risikomanagementrahmen nach dieser Verordnung unterliegen, sollten von der Verpflichtung ausgenommen werden, erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis bedrohungsorientierter Penetrationstests (TLPT — Threat Led Penetration Testing) durchzuführen, da nur Finanzunternehmen, die die Kriterien in dieser Verordnung erfüllen, verpflichtet sein sollten, diese Tests durchzuführen. Angesichts ihrer begrenzten Kapazitäten sollten Kleinstunternehmen mit dem IKT-Drittdienstleister vereinbaren können, die Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens an einen vom IKT-Drittdienstleister zu beauftragenden unabhängigen Dritten zu delegieren, sofern das Finanzunternehmen jederzeit alle relevanten Informationen und Zusicherungen über die Leistung des IKT-Drittdienstleisters von dem jeweiligen unabhängigen Dritten anfordern kann.

(44) Da nur die Finanzunternehmen, die für die Zwecke der erweiterten Tests der digitalen Resilienz bestimmt wurden, zu bedrohungsorientierten Penetrationstests verpflichtet werden sollten, sollten die Verwaltungsverfahren und finanziellen Kosten, die mit der Durchführung dieser Tests verbunden sind, von einem kleinen Prozentsatz der Finanzunternehmen getragen werden.

(45) Um die vollständige Abstimmung und allgemeine Kohärenz zwischen den Geschäftsstrategien der Finanzunternehmen einerseits und der Durchführung des IKT-Risikomanagements andererseits zu gewährleisten, sollten die Leitungsorgane der Finanzunternehmen verpflichtet sein, beim Management und bei der Anpassung des IKT-Risikomanagementrahmens und der Gesamtstrategie für die digitale operationale Resilienz eine zentrale und aktive Rolle zu bewahren. Der von den Leitungsorganen heranzuziehende Ansatz sollte sich nicht nur auf die Mittel zur Gewährleistung der Resilienz der IKT-Systeme konzentrieren, sondern auch Menschen und Prozesse durch eine Reihe von Leit- und Richtlinien einbeziehen, die auf jeder Unternehmensebene und bei allen Mitarbeitern ein starkes Bewusstsein für Cyberrisiken und die Verpflichtung zur Einhaltung einer strengen Cyberhygiene auf allen Ebenen hervorrufen. Die letztliche Verantwortung des Leitungsorgans für das Management des IKT-Risikos eines Finanzunternehmens sollte in einem übergeordneten Prinzip dieses umfassenden Ansatzes bestehen, das sich weiter im kontinuierlichen Engagement des Leitungsorgans bei der Kontrolle der Überwachung des IKT-Risikomanagements niederschlägt.

(46) Darüber hinaus geht der Grundsatz der uneingeschränkten und letztlichen Verantwortung des Leitungsorgans für das Management der IKT-Risiken des Finanzunternehmens mit der Notwendigkeit einher, einen bestimmten Umfang von IKT-Investitionen und ein Gesamtbudget sicherzustellen, die das Finanzunternehmen in die Lage versetzen, ein hohes Niveau an digitaler operationaler Resilienz zu erreichen.

(47) Aufbauend auf einschlägigen internationalen, nationalen und branchenspezifischen bewährten Verfahren, Leitlinien, Empfehlungen und Konzepten für das Management von Cyberrisiken werden mit dieser Verordnung eine Reihe von Prinzipien gefördert, die die allgemeine Struktur des IKT-Risikomanagements erleichtern. Solange die wichtigsten von Finanzunternehmen eingerichteten Kapazitäten die verschiedenen in dieser Verordnung vorgesehenen Aufgaben im IKT-Risikomanagement (Ermittlung, Schutz und Prävention, Erkennung, Reaktion und Wiederherstellung, Lernen sowie Weiterentwicklung und Kommunikation) angehen, sollte es den Finanzunternehmen folglich freistehen, IKT-Risikomanagementmodelle zu verwenden, die anders gegliedert oder kategorisiert sind.

(48) Um mit einer sich rasch ändernden Bedrohungslage Schritt zu halten, sollten Finanzunternehmen auf dem neuesten Stand befindliche IKT-Systeme unterhalten, die zuverlässig sind und nicht nur die Verarbeitung der für die Erbringung ihrer Dienste erforderlichen Daten, sondern auch ausreichende technologische Resilienz gewährleisten können, damit Finanzunternehmen in angemessener Weise auf zusätzliche Verarbeitungserfordernisse aufgrund angespannter Marktbedingungen oder anderer ungünstiger Umstände reagieren können.

(49) Effiziente Pläne zur Fortführung der Geschäftstätigkeit und für die Wiederherstellung sind erforderlich, damit Finanzunternehmen IKT-bezogenen Vorfällen, insbesondere Cyberangriffen, prompt und zügig entgegenwirken können, indem Schäden begrenzt werden und die Wiederaufnahme von Tätigkeiten und Maßnahmen für die Wiederherstellung im Einklang mit ihren Richtlinien für Datensicherung Vorrang erhalten. Eine solche Wiederaufnahme sollte jedoch die Integrität und Sicherheit der Netzwerk- und Informationssysteme oder die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten in keiner Weise gefährden.

(50) Mit dieser Verordnung wird Finanzunternehmen zwar ermöglicht, ihre Vorgaben für die Wiederherstellungszeit (recovery time objective) und die Wiederherstellungspunkte (recovery point objective) flexibel und daher so festzulegen, dass Art und Kritikalität der jeweiligen Funktion sowie etwaige spezifische geschäftliche Erfordernisse in vollem Umfang berücksichtigt werden, allerdings sollte bei der Festlegung dieser Vorgaben auch die Durchführung einer Bewertung der potenziellen Gesamtauswirkungen auf die Markteffizienz vorgeschrieben sein.

(51) Die Urheber von Cyberangriffen neigen dazu, finanzielle Gewinne direkt an der Quelle zu erzielen, sodass Finanzunternehmen weitreichenden Folgen ausgesetzt sind. Um zu verhindern, dass IKT-Systeme ihre Integrität einbüßen oder nicht verfügbar werden, und somit zu vermeiden, dass vertrauliche Daten eingesehen oder physische IKT-Infrastrukturen beschädigt werden, sollte die Meldung schwerwiegender IKT-bezogener Vorfälle durch Finanzunternehmen erheblich verbessert und gestrafft werden. Die Meldung IKT-bezogener Vorfälle sollte für alle Finanzunternehmen harmonisiert werden, indem sie verpflichtet werden, ihren jeweils zuständigen Behörden direkt Bericht zu erstatten. Unterliegt ein Finanzunternehmen der Aufsicht von mehr als einer zuständigen nationalen Behörde, so sollten die Mitgliedstaaten eine einzige zuständige Behörde als Adressat einer solchen Meldung benennen. Kreditinstitute, die gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 des Rates ([19]) als bedeutend eingestuft werden, sollten die Meldungen den zuständigen nationalen Behörden übermitteln, die sie anschließend an die Europäische Zentralbank (EZB) weiterleiten sollten.

(52) Die direkte Meldung sollte Finanzaufsichtsbehörden den direkten Zugang zu Informationen über schwerwiegende IKT-bezogene Vorfälle ermöglichen. Finanzaufsichtsbehörden sollten Einzelheiten über schwerwiegende IKT-bezogene Vorfälle wiederum an Nicht-Finanzbehörden (z. B gemäß der Richtlinie (EU) 2022/2555 benannte zuständige Behörden und zentrale Anlaufstellen, nationale Datenschutzbehörden und Strafverfolgungsbehörden bei schwerwiegenden IKT-bezogenen Vorfällen strafrechtlicher Art) weiterleiten, um diese Behörden für diese Vorfälle zu sensibilisieren und bei CSIRT gegebenenfalls die unverzügliche Unterstützung von Finanzunternehmen zu erleichtern. Darüber hinaus sollten die Mitgliedstaaten festlegen können, dass Finanzunternehmen selbst derartige Informationen an Behörden außerhalb des Finanzdienstleistungsbereichs weitergeben sollten. Diese Informationsflüsse sollten es Finanzunternehmen ermöglichen, rasch von allen einschlägigen technischen Informationen, der Beratung über Abhilfemaßnahmen und den anschließenden Folgemaßnahmen dieser Behörden zu profitieren. Die Informationen über schwerwiegende IKT-bezogene Vorfälle sollten wechselseitig gelenkt werden: Die Finanzaufsichtsbehörden sollten dem Finanzunternehmen alle erforderlichen Rückmeldungen oder Orientierungshilfen geben, während die ESA anonymisierte Daten über Cyberbedrohungen und Schwachstellen im Zusammenhang mit einem Vorfall austauschen sollten, um eine umfassende kollektive Verteidigung zu unterstützen.

(53) Zwar sollten alle Finanzunternehmen verpflichtet sein, Sicherheitsvorfälle zu melden, es ist jedoch davon auszugehen, dass diese Verpflichtung sie nicht alle in gleicher Weise betrifft. Die einschlägigen Wesentlichkeitsschwellen sowie die Fristen für die Meldung sollten im Rahmen delegierter Rechtsakte auf der Grundlage der von den ESA zu entwickelnden technischen Regulierungsstandards gebührend angepasst werden, um nur schwerwiegende IKT-bezogene Vorfälle abzudecken. Darüber hinaus sollten die Besonderheiten von Finanzunternehmen bei der Festlegung der Fristen für die Meldepflichten berücksichtigt werden.

(54) Diese Verordnung sollte Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister und E-Geld-Institute verpflichten, alle zuvor gemäß der Richtlinie (EU) 2015/2366 gemeldeten zahlungsbezogenen Betriebs- oder Sicherheitsvorfälle zu melden, unabhängig von der Art des IKT-Vorfalls.

([19]) Verordnung (EU) Nr. 1024/2013 des Rates vom 15. Oktober 2013 zur Übertragung besonderer Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute auf die Europäische Zentralbank (ABl. L 287 vom 29.10.2013, S. 63).

(55) Die ESA sollten beauftragt werden, die Durchführbarkeit und die Bedingungen für eine mögliche Zentralisierung von Meldungen über IKT-bezogene Vorfälle auf Unionsebene zu bewerten. Eine solche Zentralisierung könnte in einer einheitlichen EU-Plattform für die Meldung schwerwiegender IKT-bezogener Vorfälle bestehen, die die entsprechenden Meldungen entweder direkt entgegennimmt und die zuständigen nationalen Behörden automatisch benachrichtigt oder lediglich die von den zuständigen nationalen Behörden übermittelten einschlägigen Meldungen zentralisiert und somit eine Koordinierungsfunktion wahrnimmt. Die ESA sollten beauftragt werden, in Absprache mit der EZB und der ENISA einen gemeinsamen Bericht über die Machbarkeit der Einrichtung einer einheitlichen EU-Plattform auszuarbeiten.

(56) Um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen und im Einklang sowohl mit den einschlägigen internationalen Standards (z. B. die „G7 Fundamental Elements for Threat-Led Penetration Testing“ (Grundzüge bedrohungsorientierter Penetrationstests der G7-Staaten)) als auch den in der Union angewandten Rahmen (z. B. TIBER-EU), sollten Finanzunternehmen ihre IKT-Systeme und ihre Mitarbeiter mit IKT-bezogenen Verantwortungen regelmäßig auf die Effizienz ihrer Fähigkeiten für Prävention, Erkennung, Reaktion und Wiederherstellung hin testen, um potenzielle IKT-Schwachstellen aufzudecken und zu beseitigen. Um den Unterschieden Rechnung zu tragen, die zwischen und in den verschiedenen Finanzteilsektoren bei der Abwehrbereitschaft von Finanzunternehmen im Bereich der Cybersicherheit bestehen, sollten die Tests eine breite Palette von Instrumenten und Maßnahmen umfassen, die von der Bewertung grundlegender Anforderungen (z. B. Bewertungen und Überprüfungen der Schwachstellen, Analysen von Open-Source-Software, Bewertungen der Netzwerksicherheit, Lückenanalysen, Analysen der physischen Sicherheit, Fragebögen und Scansoftwarelösungen, Quellcodeprüfungen, soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests oder End-to-End-Tests) bis hin zu erweiterten Tests anhand von TLPT reichen. Diese erweiterten Tests sollten nur für Finanzunternehmen vorgeschrieben werden, die aus IKT-Perspektive ausgereift genug sind, um sie angemessen durchführen zu können. Folglich sollten die in dieser Verordnung vorgeschriebene Tests der digitalen operationalen Resilienz für die Finanzunternehmen, die die Kriterien dieser Verordnung erfüllen (zum Beispiel große systemrelevante Kreditinstitute mit ausgereifter IKT, Börsen, Zentralverwahrer und zentrale Gegenparteien), ausgedehnter sein als für andere Finanzunternehmen. Gleichzeitig sollten die Tests der digitalen operationalen Resilienz anhand von TLPT für Finanzunternehmen, die in zentralen Finanzdienstleistungsteilsektoren tätig sind und eine systemrelevante Rolle spielen (zum Beispiel Zahlungen, Banken sowie Clearing und Abrechnung), mehr Relevanz und für andere Teilsektoren (zum Beispiel Vermögensverwalter, Ratingagenturen usw.) weniger Relevanz besitzen.

(57) Grenzübergreifend tätige Finanzunternehmen, die die Niederlassungs- oder Dienstleistungsfreiheit in der Union ausüben, sollten in ihrem Herkunftsmitgliedstaat eine einheitliche Reihe von Anforderungen für erweiterte Tests (z. B. TLPT) erfüllen, die sich auf die IKT-Infrastrukturen in allen Rechtsordnungen erstrecken sollten, in denen die grenzüberschreitende Finanzgruppe innerhalb der Union tätig ist, sodass diesen grenzüberschreitend tätigen Finanzgruppen nur in einer Rechtsordnung entsprechende IKT-bezogene Testkosten entstehen.

(58) Um das Fachwissen zu nutzen, das bestimmte zuständige Behörden bereits erworben haben, insbesondere im Zusammenhang mit der Umsetzung von TIBER-EU, sollte es den Mitgliedstaaten durch diese Verordnung ermöglicht werden, auf nationaler Ebene eine einzige staatliche Behörde zu benennen, die im Finanzsektor für alle TLPT-bezogenen Fragen zuständig ist, oder — falls keine solche Behörde benannt wurde — die entsprechenden zuständigen Behörden zu benennen, die die Wahrnehmung von TLPT-bezogenen Aufgaben einer anderen zuständigen nationalen Finanzbehörde übertragen.

(59) Da Finanzunternehmen nach dieser Verordnung nicht verpflichtet sind, mit einem einzigen bedrohungsorientierten Penetrationstest alle kritischen oder wichtigen Funktionen abzudecken, sollte es den Finanzunternehmen freistehen, jeweils festzulegen, welche und wie viele kritische oder wichtige Funktionen im Rahmen dieser Tests geprüft werden sollten.

(60) Gebündelte Tests im Sinne dieser Verordnung — bei denen verschiedene Finanzunternehmen an einem TLPT teilnehmen und ein IKT-Drittdienstleister zu diesem Zweck direkt vertragliche Vereinbarungen mit einem externen Tester eingehen kann — sollten nur dann zulässig sein, wenn gerechtfertigt von nachteiligen Auswirkungen auf die Qualität oder Sicherheit derjenigen Dienstleistungen ausgegangen werden kann, die der IKT-Drittdienstleister für Kunden erbringt, bei denen es sich um nicht in den Geltungsbereich dieser Verordnung fallende Unternehmen handelt, oder auf die Vertraulichkeit von mit diesen Dienstleistungen in Verbindung stehenden Daten. Gebündelte Tests sollten auch Schutzvorkehrungen unterliegen (Leitung durch ein benanntes Finanzunternehmen, Abgleich der Anzahl der teilnehmenden Finanzunternehmen), damit ein strenges Testverfahren für diejenigen beteiligten Finanzunternehmen gewährleistet ist, die den Zielen des TLPT gemäß dieser Verordnung gerecht werden.

(61) Um die auf Unternehmensebene verfügbaren internen Ressourcen zu nutzen, sollte der Einsatz interner Tester zur Durchführung von TLPT gemäß dieser Verordnung gestattet sein, sofern eine aufsichtliche Genehmigung vorliegt, keine Interessenkonflikte bestehen und ein regelmäßiger Wechsel (jeweils nach drei Tests) im Einsatz von internen und externen Testern stattfindet, wobei es sich zudem bei dem Anbieter der Bedrohungsanalyse im Rahmen der TLPT stets um ein Unternehmen außerhalb des betreffenden Finanzunternehmens handeln muss. Die Durchführung von TLPT sollten weiterhin uneingeschränkt in der Verantwortung der Finanzunternehmen liegen. Die von den Behörden ausgestellten Bescheinigungen sollten ausschließlich dem Zweck der gegenseitigen Anerkennung dienen und sollten weder Folgemaßnahmen ausschließen, die erforderlich sind, um IKT-Risiken, denen das Finanzunternehmen ausgesetzt ist, anzugehen, noch sollten sie als aufsichtliche Billigung der IKT-Risikomanagement- und -minderungsfähigkeiten eines Finanzunternehmens betrachtet werden.

(62) Um eine solide Überwachung des IKT-Drittparteienrisikos im Finanzsektor zu gewährleisten, sind eine Reihe grundsatzbasierter Regeln festzulegen, um Finanzunternehmen bei der Überwachung der Risiken anzuleiten, die im Zusammenhang mit an IKT-Drittdienstleister ausgelagerten Funktionen — insbesondere mit IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen — sowie ganz allgemein im Zusammenhang mit jeglichen Abhängigkeiten von IKT-Drittdienstleistern entstehen.

(63) Um der Komplexität der verschiedenen IKT-Risikoquellen und dabei zugleich der Vielzahl und Vielfalt der Anbieter technologischer Lösungen, die eine reibungslose Erbringung von Finanzdienstleistungen ermöglichen, gerecht zu werden, sollte diese Verordnung für ein breites Spektrum von IKT-Drittdienstleistern gelten, darunter Anbieter von Cloud-Computing-Diensten, Software, Datenanalysediensten und Anbieter von Rechenzentrumsdienstleistungen. Da Finanzunternehmen alle Arten von Risiken — auch im Zusammenhang mit innerhalb einer Finanzgruppe beschafften IKT-Dienstleistungen — wirksam und kohärent ermitteln und managen sollten, sollte zudem klar herausgestellt werden, dass Unternehmen, die Teil einer Finanzgruppe sind und IKT-Dienstleistungen vorwiegend für ihr Mutterunternehmen oder für Tochterunternehmen oder Zweigniederlassungen ihres Mutterunternehmens erbringen, sowie Finanzunternehmen, die IKT-Dienstleistungen für andere Finanzunternehmen erbringen, ebenfalls als IKT-Drittdienstleister im Sinne dieser Verordnung gelten sollten. Angesichts der zunehmenden Abhängigkeit des sich entwickelnden Marktes für Zahlungsdienste von komplexen technischen Lösungen sowie angesichts neu entstehender Arten von Zahlungsdiensten und zahlungsbezogenen Lösungen sollten diejenigen Teilnehmer des Ökosystems für Zahlungsdienste, die Zahlungsabwicklungstätigkeiten durchführen oder Zahlungsinfrastrukturen betreiben, ebenfalls als IKT-Drittdienstleister im Sinne dieser Verordnung gelten, mit Ausnahme von Zentralbanken, die Zahlungs- oder Wertpapierliefer- und -abrechnungssysteme betreiben, und von staatlichen Behörden, die IKT-bezogene Dienste im Zusammenhang mit Funktionen des Staates bereitstellen.

(64) Ein Finanzunternehmen sollte jederzeit die volle Verantwortung für die Einhaltung seiner Verpflichtungen aus dieser Verordnung tragen. Die Finanzunternehmen sollten bei der Überwachung der Risiken, die auf Ebene der IKT-Drittdienstleister entstehen, einen verhältnismäßigen Ansatz verfolgen, indem Art, Umfang, Komplexität und Bedeutung ihrer IKT-bezogener Abhängigkeiten und die Kritikalität oder Bedeutung der Dienste, Prozesse oder Funktionen, die den vertraglichen Vereinbarungen unterliegen, letztlich je nach Sachlage anhand einer sorgfältigen Bewertung jeglicher potenzieller Auswirkungen auf die Kontinuität und Qualität von Finanzdienstleistungen auf Einzel- und Gruppenebene gebührend berücksichtigt werden.

(65) Die Durchführung einer solchen Überwachung sollte nach einem strategischen Ansatz für das IKT-Drittparteienrisiko erfolgen, der durch die Annahme einer eigenen Strategie für das von IKT-Drittdienstleistern ausgehende Risiko durch das Leitungsorgan des Finanzunternehmens formalisiert wird, und zwar auf der Grundlage einer kontinuierlichen Überprüfung aller Abhängigkeiten von IKT-Drittdienstleistern. Um die Aufsichtsbehörden für Abhängigkeiten von IKT-Drittdienstleistern zu sensibilisieren und die Arbeiten im Zusammenhang mit dem durch diese Verordnung geschaffenen Überwachungsrahmen weiter zu unterstützen, sollten sämtliche Finanzunternehmen verpflichtet werden, ein Informationsregister mit allen vertraglichen Vereinbarungen betreffend die Nutzung von IKT-Dienstleistungen, die von IKT-Drittdienstleistern bereitgestellt werden, zu führen. Die Finanzaufsichtsbehörden sollten in der Lage sein, das vollständige Register oder bestimmte Abschnitte des Registers anzufordern und somit wesentliche Informationen zu erhalten, die ein umfassenderes Verständnis der IKT-bezogenen Abhängigkeiten von Finanzunternehmen ermöglichen.

(66) Dem förmlichen Abschluss vertraglicher Vereinbarungen sollte eine gründliche Analyse vor Vertragsabschluss zugrunde liegen und diesem vorausgehen, insbesondere indem der Fokus auf Aspekte wie die Kritikalität oder Bedeutung der durch den geplanten IKT-Vertrag unterstützten Dienste, die erforderlichen aufsichtlichen Genehmigungen oder sonstigen Bedingungen, das damit verbundene mögliche Konzentrationsrisiko sowie die Anwendung der Sorgfaltspflicht bei der Auswahl und Bewertung von IKT-Drittdienstleistern gelegt wird, und indem potenzielle Interessenkonflikte bewertet werden. Betreffen vertragliche Vereinbarungen kritische oder wichtige Funktionen, so sollten Finanzunternehmen darauf achten, dass IKT-Drittdienstleister die aktuellsten und höchsten Standards für die Informationssicherheit anwenden. Die Kündigung vertraglicher Vereinbarungen könnte zumindest

durch eine Reihe von Umständen ausgelöst werden, die Unzulänglichkeiten auf Ebene des IKT-Drittdienstleister erkennen lassen, insbesondere erhebliche Verstöße gegen Rechtsvorschriften oder Vertragsbestimmungen, Umstände, die auf eine potenzielle Änderung der Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen hindeuten, Hinweise auf Schwachstellen beim allgemeinen IKT-Risikomanagement des IKT-Drittdienstleisters oder Umstände, die darauf hinweisen, dass die jeweils zuständige Behörde nicht zu einer wirksamen Beaufsichtigung des Finanzunternehmens in der Lage sind.

(67) Um die systemischen Auswirkungen des Konzentrationsrisikos von IKT-Drittdienstleistern zu anzugehen, wird mit dieser Verordnung eine ausgewogene Lösung angestrebt, indem bei solchen Konzentrationsrisiken ein flexibler und schrittweiser Ansatz verfolgt wird, da jegliche vorgeschriebene starre Obergrenzen oder strenge Beschränkungen die Geschäftstätigkeit behindern und die Vertragsfreiheit beeinträchtigen können. Finanzunternehmen sollten ihre geplanten vertraglichen Vereinbarungen gründlich prüfen, um die Wahrscheinlichkeit des Auftretens eines solchen Risikos zu ermitteln, unter anderem durch fundierte Analysen von Unterauftragsvereinbarungen, insbesondere wenn diese mit IKT-Drittdienstleistern geschlossen werden, die in einem Drittland niedergelassen sind. Um ein ausgewogenes Verhältnis zwischen dem Sachzwang, zum einen die Vertragsfreiheit zu wahren und zum anderen die Finanzstabilität zu gewährleisten, wird es zum gegenwärtigen Zeitpunkt nicht als zweckmäßig erachtet, strenge Obergrenzen und Beschränkungen für die Exposition gegenüber IKT-Drittdienstleistern festzulegen. Was kritische IKT-Drittdienstleister anbelangt, so sollte eine nach dieser Verordnung ernannte federführende Überwachungsbehörde bei der Wahrnehmung ihrer Aufsichtsaufgaben im Kontext des Überwachungsrahmens besonders darauf achten, das Ausmaß der Interdependenzen voll zu erfassen, spezifische Fälle zu ermitteln, in deren Rahmen eine hohe Konzentration kritischer IKT-Drittdienstleister in der Union die Stabilität und Integrität des Finanzsystems der Union belasten dürfte, sowie einen Dialog mit kritischen IKT-Drittdienstleistern zu führen, bei denen dieses spezifische Risiko ermittelt wird.

(68) Um die Fähigkeit eines IKT-Drittdienstleisters, sichere Dienstleistungen für ein Finanzunternehmen ohne nachteilige Auswirkungen auf dessen digitale operationale Resilienz zu erbringen, regelmäßig zu bewerten und zu überwachen, sollten einige wesentliche Vertragsbestandteile mit IKT-Drittdienstleistern harmonisiert werden. Diese Harmonisierung sollte Mindestbereiche abdecken, die — unter dem Gesichtspunkt, dass ein Finanzunternehmen seine digitale Resilienz sicherstellen muss, da es in hohem Maße von der Stabilität, der Funktionalität, der Verfügbarkeit und der Sicherheit der beanspruchten IKT-Dienstleistungen abhängig ist — für eine umfassende Überwachung der von einem IKT-Drittdienstleister möglicherweise ausgehenden Risiken durch das Finanzunternehmen von entscheidender Bedeutung sind.

(69) Bei der Neuaushandlung vertraglicher Vereinbarungen zwecks Angleichung an die Anforderungen dieser Verordnung sollten Finanzunternehmen und IKT-Drittdienstleister sicherstellen, dass die in dieser Verordnung vorgesehenen wesentlichen Vertragsbestimmungen berücksichtigt werden.

(70) Die Begriffsbestimmung der „kritischen oder wichtigen Funktion“ im Sinne dieser Verordnung schließt auch die Begriffsbestimmung der „kritischen Funktionen“ im Sinne von Artikel 2 Absatz 1 Nummer 35 der Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates ([20]) ein. Dementsprechend sind die gemäß der Richtlinie 2014/59/EU als kritisch eingestuften Funktionen in der Begriffsbestimmung der kritischen Funktionen im Sinne dieser Verordnung ebenfalls erfasst.

(71) Ungeachtet der Kritikalität oder Bedeutung der von dem IKT-Drittdienstleister unterstützten Funktion sollte in den vertraglichen Vereinbarungen insbesondere eine Spezifikation der vollständigen Beschreibungen von Funktionen und Dienstleistungen sowie von Orten, an denen solche Funktionen bereitgestellt werden und Daten verarbeitet werden sollen, vorgesehen sein; ferner sollten Beschreibungen der Dienstleistungsgüte enthalten sein. Andere wesentliche Elemente um einem Finanzunternehmen die Überwachung des IKT-Drittparteienrisikos zu ermöglichen, sind die Folgenden: vertragliche Bestimmungen dazu, wie Zugänglichkeit, Verfügbarkeit, Integrität, Sicherheit und Schutz personenbezogener Daten durch den IKT-Drittdienstleister gewährleistet werden; Bestimmungen über die einschlägigen Garantien für den Zugang zu sowie die Wiederherstellung und Rückgabe von Daten im Falle einer Insolvenz, Abwicklung oder Einstellung der Geschäftstätigkeit des IKT-Drittdienstleisters; Bestimmungen, die den IKT-Drittdienstleister dazu verpflichten, im Falle von IKT-Vorfällen im Zusammenhang mit den erbrachten Dienstleistungen ohne zusätzliche Kosten oder zu vorab festzusetzenden Kosten Unterstützung zu

([20]) Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 zur Festlegung eines Rahmens für die Sanierung und Abwicklung von Kreditinstituten und Wertpapierfirmen und zur Änderung der Richtlinie 82/891/EWG des Rates, der Richtlinien 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU und 2013/36/EU sowie der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates (ABl. L 173 vom 12.6.2014, S. 190).

leisten; Bestimmungen über die Verpflichtung des IKT-Drittdienstleisters, uneingeschränkt mit den für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden zusammenzuarbeiten, sowie Bestimmungen über Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechend den Erwartungen der zuständigen Behörden und Abwicklungsbehörden.

(72) In Ergänzung zu derartigen vertraglichen Bestimmungen sowie um sicherzustellen, dass Finanzunternehmen die volle Kontrolle über alle von Dritten ausgehenden Entwicklungen behalten, die ihre IKT-Sicherheit beeinträchtigen könnten, sollten die Verträge über die Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen zudem Folgendes vorschreiben: die Spezifikation der vollständigen Beschreibung der Dienstleistungsgüte einschließlich präziser quantitativer und qualitativer Leistungsziele, damit unverzüglich angemessene Korrekturmaßnahmen ergriffen werden können, wenn die vereinbarte Dienstleistungsgüte nicht erreicht werden; die einschlägigen Kündigungsfristen und Meldepflichten des IKT-Drittdienstleisters im Falle von Entwicklungen, die sich wesentlich auf die Fähigkeit des IKT-Drittdienstleisters auswirken könnten, die entsprechenden IKT-Dienstleistungen wirksam zur Verfügung stellen; die Anforderung an den IKT-Drittdienstleister, Notfallpläne zu implementieren und zu erproben und über Maßnahmen, Instrumente und Leit- und Richtlinien für IKT-Sicherheit zu verfügen, die eine sichere Erbringung von Dienstleistungen ermöglichen, sowie sich an dem TLPT des Finanzunternehmens zu beteiligen und uneingeschränkt daran mitzuwirken.

(73) Verträge über die Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sollten zudem Bestimmungen enthalten, die Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens oder eines beauftragten Dritten sowie das Recht auf Anfertigung von Kopien regeln, die als wesentliche Instrumente für die laufende Überwachung der Leistung des IKT-Drittdienstleisters durch die Finanzunternehmen dienen, gepaart mit der uneingeschränkten Zusammenarbeit des Drittdienstleisters während der Inspektionen. In gleicher Weise sollte die für das Finanzunternehmen zuständige Behörde auf der Grundlage von Mitteilungen über das Recht verfügen, den IKT-Drittdienstleister vorbehaltlich des Schutzes vertraulicher Informationen zu inspizieren und zu prüfen.

(74) Diese vertraglichen Vereinbarungen sollten ferner spezielle Ausstiegsstrategien vorsehen, die insbesondere verbindliche Übergangszeiträume ermöglichen, in denen die IKT-Drittdienstleister weiterhin die einschlägigen Dienste bereitstellen sollten, um das Risiko von Störungen auf Ebene des Finanzunternehmens zu verringern oder es Letzterem zu ermöglichen, effektiv zu anderen IKT-Drittdienstleistern zu wechseln oder alternativ zu internen Lösungen zu wechseln, die der Komplexität der bereitgestellten IKT-Dienstleistungen entsprechen. Darüber hinaus sollten Finanzunternehmen, die in den Geltungsbereich der Richtlinie 2014/59/EU fallen, sicherstellen, dass die einschlägigen Verträge über IKT-Dienstleistungen solide und im Falle der Abwicklung dieser Finanzunternehmen uneingeschränkt durchsetzbar sind. Daher sollten diese Finanzunternehmen im Einklang mit den Erwartungen der Abwicklungsbehörden sicherstellen, dass die einschlägigen Verträge über IKT-Dienstleistungen abwicklungssicher sind. Solange diese Finanzunternehmen ihren Zahlungsverpflichtungen weiterhin nachkommen, sollten sie neben anderen Anforderungen sicherstellen, dass die einschlägigen Verträge über IKT-Dienstleistungen Klauseln darüber enthalten, dass sie nicht aufgrund einer Umstrukturierung oder Abwicklung gekündigt, ausgesetzt oder geändert werden können.

(75) Darüber hinaus kann die freiwillige Verwendung von Standardvertragsklauseln, die von staatlichen Behörden oder von Organen der Union entwickelt wurden, insbesondere die Verwendung von der Kommission für Cloud-Computing Dienste entwickelten Vertragsklauseln den Finanzunternehmen und IKT-Drittdienstleistern eine zusätzliche Rückversicherung bieten, indem sie die Rechtssicherheit in Bezug auf die Nutzung von Cloud-Computing-Diensten im Finanzsektor in voller Übereinstimmung mit den Anforderungen und Erwartungen des Finanzdienstleistungsrechts der Union erhöht. Die Erarbeitung von Standardvertragsklauseln baut auf Maßnahmen auf, die bereits im FinTech-Aktionsplan von 2018 vorgesehen waren, in dem die Absicht der Kommission angekündigt wurde, die Entwicklung von Standardvertragsklauseln für die Auslagerung von Cloud-Computing-Dienstleistungen durch Finanzunternehmen zu fördern und zu erleichtern, wobei auf den sektorübergreifenden Anstrengungen der Cloud-Interessenträger aufgebaut wird, die die Kommission unter Beteiligung des Finanzsektors unterstützt hat.

(76) Um die Konvergenz und Effizienz von Aufsichtskonzepten in Bezug auf das IKT-Drittparteienrisiko im Finanzsektor zu fördern und um die digitale operationale Resilienz von Finanzunternehmen zu stärken, die bei den IKT-Dienstleistungen, die die Erbringung von Finanzdienstleistungen unterstützen, auf kritische IKT-Drittdienstleister angewiesen sind, und damit zugleich dazu beizutragen, die Stabilität des Finanzsystems der Union und die Integrität des Binnenmarkts für Finanzdienstleistungen zu bewahren, sollten kritische IKT-Drittdienstleister einem Überwachungsrahmen der Union unterliegen. Auch wenn die Einrichtung des Überwachungsrahmens aufgrund des Mehrwerts von Maßnahmen auf Unionsebene und der inhärenten Rolle und der Besonderheiten der Nutzung von

IKT-Dienstleistungen bei der Erbringung von Finanzdienstleistungen gerechtfertigt ist, sollte zugleich daran erinnert werden, dass diese Lösung nur im Kontext dieser Verordnung, die speziell der digitalen operationalen Resilienz im Finanzsektor vorbehalten ist, angemessen erscheint. Ein solcher Überwachungsrahmen sollte hingegen nicht als ein neues Modell für die Beaufsichtigung auf Ebene der Union in den Bereichen Finanzdienstleistungen und -tätigkeiten betrachtet werden.

(77) Der Überwachungsrahmen sollte nur für kritische IKT-Drittdienstleister gelten. Daher sollte es einen Einstufungsmechanismus geben, um dem Ausmaß und der Art der Abhängigkeit des Finanzsektors von solchen IKT-Drittdienstleistern Rechnung zu tragen. Dieser Mechanismus sollte eine Reihe quantitativer und qualitativer Kriterien umfassen, mit denen die Kritikalitätsparameter als Grundlage für die Einbeziehung in den Überwachungsrahmen festgelegt würden. Um eine akkurate Bewertung zu gewährleisten, sollten diese Kriterien unabhängig von der Unternehmensstruktur des IKT-Drittdienstleisters im Falle eines IKT-Drittdienstleisters, der Teil einer größeren Gruppe ist, die gesamte Gruppenstruktur des IKT-Drittdienstleisters berücksichtigen. Einerseits sollten kritische IKT-Drittdienstleister, die aufgrund der Anwendung der oben genannten Kriterien nicht automatisch eingestuft werden, die Möglichkeit haben, sich auf freiwilliger Basis für den Überwachungsrahmen zu entscheiden, andererseits sollten IKT-Drittdienstleister, die bereits Überwachungsmechanismen unterliegen, die die Erfüllung der in Artikel 127 Absatz 2 AEUV genannten Aufgaben des Europäischen Systems der Zentralbanken unterstützen, ausgenommen werden.

(78) Ebenso sollten Finanzunternehmen, die IKT-Dienstleistungen für andere Finanzunternehmen bereitstellen, zugleich aber der von dieser Verordnung erfassten Kategorie von IKT-Drittdienstleistern angehören, ebenfalls von dem Überwachungsrahmen ausgenommen werden, da sie bereits den Aufsichtsmechanismen unterliegen, die durch das einschlägige Finanzdienstleistungsrecht der Union geschaffen wurden. Wenn zweckmäßig sollten die zuständigen Behörden im Rahmen ihrer Aufsichtstätigkeiten das IKT-Risiko berücksichtigen, das von den IKT-Dienstleistungen bereitstellenden Finanzunternehmen für andere Finanzunternehmen ausgeht. In gleicher Weise sollte aufgrund der auf Gruppenebene bestehenden Risikoüberwachungsmechanismen dieselbe Ausnahme für diejenigen IKT-Drittdienstleister vorgesehen werden, die Dienstleistungen vorwiegend für die ihrer eigenen Gruppe angehörenden Unternehmen erbringen. IKT-Drittdienstleister, die lediglich in einem Mitgliedstaat IKT-Dienstleistungen für Finanzunternehmen bereitstellen, die nur in diesem Mitgliedstaat tätig sind, sollten aufgrund ihrer begrenzten Tätigkeiten und der fehlenden grenzüberschreitenden Auswirkungen ebenfalls von dem Einstufungsmechanismus ausgenommen werden.

(79) Der digitale Wandel im Bereich der Finanzdienstleistungen hat zu einem noch nie da gewesenen Maß an Nutzung und Abhängigkeit von IKT-Dienstleistungen geführt. Da es unvorstellbar geworden ist, Finanzdienstleistungen ohne die Nutzung von Cloud-Computing-Diensten, Softwarelösungen und datenbezogenen Dienstleistungen zu erbringen, ist das Finanzökosystem der Union zwangsläufig immer abhängiger von bestimmten IKT-Dienstleistungen geworden, die von IKT-Dienstleistern bereitgestellt werden. Einige dieser Dienstleister sind Innovatoren bei der Entwicklung und Anwendung IKT-gestützter Technologien und spielen daher eine wichtige Rolle bei der Erbringung von Finanzdienstleistungen oder sind nunmehr fester Bestandteil der Wertschöpfungskette für Finanzdienstleistungen geworden. Somit sind sie für die Stabilität und Integrität des Finanzsystems der Union inzwischen von entscheidender Bedeutung. Diese breite Abhängigkeit von Dienstleistungen, die von kritischen IKT-Drittdienstleistern erbracht werden, in Verbindung mit der Interdependenz der Informationssysteme verschiedener Marktteilnehmer schafft ein unmittelbares und potenziell schwerwiegendes Risiko für das Finanzdienstleistungssystem der Union und für die Kontinuität bei der Erbringung von Finanzdienstleistungen, falls kritische IKT-Drittdienstleister von Betriebsstörungen oder schwerwiegenden Cybervorfällen betroffen sein sollten. Cybervorfälle haben die Besonderheit, dass sie sich im gesamten Finanzsystem potenzieren und erheblich schneller verbreiten können als andere Arten von Risiken, die im Finanzsektor überwacht werden, und sich über Branchen und geografische Grenzen hinweg ausbreiten können. Sie haben das Potenzial, sich zu einer Systemkrise auszuweiten, bei der das Vertrauen in das Finanzsystem aufgrund der Unterbrechung von Funktionen zur Stützung der Realwirtschaft oder aufgrund erheblicher finanzieller Verluste auf ein Niveau sinkt, dem das Finanzsystem nicht standhalten kann oder das gezielte Maßnahmen zur Abfederung schwerer Schocks erfordert. Um zu verhindern, dass diese Szenarien eintreten und dabei die Stabilität und Integrität des Finanzsystems der Union gefährden, ist es von entscheidender Bedeutung, die Aufsichtspraktiken hinsichtlich des IKT-Drittparteienrisikos im Finanzsektor einander anzunähern, insbesondere durch neue Vorschriften, die die Überwachung kritischer IKT-Drittdienstleister in der Union ermöglichen.

(80) Der Überwachungsrahmen hängt weitgehend vom Ausmaß der Zusammenarbeit zwischen der federführenden Überwachungsbehörde und dem kritischen IKT-Drittdienstleister ab, der Dienste für Finanzunternehmen bereitstellt, die sich auf die Erbringung von Finanzdienstleistungen auswirken. Eine erfolgreiche Überwachung setzt unter anderem voraus, dass die federführende Überwachungsbehörde in der Lage ist, Überwachungsmissionen und Inspektionen effektiv durchzuführen, um die von kritischen IKT-Drittdienstleistern angewandten Regeln, Kontrollen und Verfahren sowie die potenziellen kumulativen Auswirkungen ihrer Tätigkeiten auf die Finanzstabilität und die Integrität des Finanzsystems zu bewerten. Gleichzeitig ist es entscheidend, dass kritische IKT-Drittdienstleister die Empfehlungen der federführenden Überwachungsbehörde befolgen und deren Bedenken ausräumen. Da ein kritischer IKT-Drittdienstleister, der Dienste bereitstellt, die sich auf die Erbringung von Finanzdienstleistungen auswirken, durch seine mangelnde Zusammenarbeit — beispielsweise indem er den Zugang zu seinen Räumlichkeiten oder die Übermittlung von Informationen verweigert — der federführenden Überwachungsbehörde letztlich ihre wichtigsten Instrumente zur Bewertung des IKT-Drittparteienrisikos nehmen würde und die Finanzstabilität und die Integrität des Finanzsystems dadurch beeinträchtigt werden könnten, ist auch eine angemessene Sanktionsregelung vorzusehen.

(81) Vor diesem Hintergrund sollte die Anforderung, dass eine federführende Überwachungsbehörde Zwangsgelder verhängen können muss, um kritische IKT-Drittdienstleister zur Einhaltung der in dieser Verordnung festgelegten Transparenz- und Zugangsverpflichtungen zu zwingen, nicht durch Schwierigkeiten gefährdet werden, die bei der Durchsetzung dieser Zwangsgelder in Bezug auf kritische IKT-Drittdienstleister mit Sitz in einem Drittland auftreten können. Um solche Sanktionen durchsetzen zu können und eine rasche Aufnahme von Verfahren zur Wahrung der Verteidigungsrechte kritischer IKT-Drittdienstleister im Zusammenhang mit dem Einstufungsmechanismus und der Herausgabe von Empfehlungen zu ermöglichen, sollten diese kritische IKT-Drittdienstleister, die Dienste für Finanzunternehmen bereitstellen, die sich auf die Erbringung von Finanzdienstleistungen auswirken, dazu verpflichtet werden, eine angemessene geschäftliche Präsenz in der Union aufrechtzuerhalten. Aufgrund der Art der Überwachung und fehlender vergleichbarer Regelungen in anderen Rechtsordnungen gibt es keine geeigneten alternativen Mechanismen, die diesem Ziel genügen, indem bei der Überwachung der Auswirkungen digitaler operationeller Risiken, die von systemrelevanten, als kritisch eingestuften IKT-Drittdienstleistern mit Sitz in einem Drittland ausgehen, effektiv mit den Finanzaufsichtsbehörden in Drittländern zusammengearbeitet wird. Um weiterhin kontinuierlich IKT-Dienstleistungen für Finanzunternehmen in der Union bereitstellen zu können, sollte ein IKT-Drittdienstleister mit Sitz in einem Drittland, der als kritisch im Sinne dieser Verordnung eingestuft worden ist, daher innerhalb von zwölf Monaten nach dieser Einstufung alle erforderlichen Vorkehrungen treffen, um seine Eingliederung in die Union mittels Gründung eines Tochterunternehmens im Sinne des Besitzstands der Union, namentlich der Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates ([21]), sicherzustellen.

(82) Die Anforderung, in der Union ein Tochterunternehmen zu gründen, sollte den kritischen IKT-Drittdienstleister nicht daran hindern, IKT-Dienstleistungen und damit verbundene technische Unterstützung von außerhalb der Union gelegenen Einrichtungen und Infrastruktur aus bereitzustellen. Diese Verordnung auferlegt keine Verpflichtung zur Lokalisierung von Daten, da sie keine Speicherung oder Verarbeitung von Daten in der Union vorschreibt.

(83) Kritische IKT-Drittdienstleister sollten in der Lage sein, IKT-Dienstleistungen von jedem beliebigen Ort der Welt aus zu erbringen, nicht unbedingt oder ausschließlich von einem in der Union gelegenen Ort aus. Die Überwachungstätigkeiten sollten zunächst an einem Ort in der Union und im Wege der Interaktion mit in der Union gelegenen Unternehmen, einschließlich der von kritischen IKT-Drittdienstleistern im Sinne dieser Verordnung gegründeten Tochterunternehmen, durchgeführt werden. Diese Maßnahmen innerhalb der Union reichen jedoch möglicherweise nicht aus, um der federführenden Überwachungsbehörde die uneingeschränkte und wirksame Wahrnehmung ihrer Aufgaben im Rahmen dieser Verordnung zu ermöglichen. Die federführende Überwachungsbehörde sollte daher ihre einschlägigen Überwachungsbefugnisse auch in Drittländern ausüben können. Durch die Ausübung dieser Befugnisse in Drittländern sollte es der federführenden Überwachungsbehörde möglich sein, die Einrichtungen zu prüfen, von denen aus die IKT-Dienstleistungen oder die technischen Unterstützungsdienste tatsächlich von dem kritischen IKT-Drittdienstleister bereitgestellt oder betrieben werden, und ein umfassendes und operatives Verständnis des IKT-Risikomanagements des kritischen IKT-Drittdienstleisters zu erhalten. Die Möglichkeit, dass die federführende Überwachungsbehörde als Agentur der Union Befugnisse außerhalb des Gebiets der Union ausübt, sollte durch Festschreibung der einschlägigen Voraussetzungen, insbesondere der Zustimmung des betreffenden kritischen IKT-Drittdienstleisters, klar geregelt werden. Ebenso sollten die einschlägigen Behörden des Drittlandes darüber unterrichtet sein, welche Tätigkeiten die federführende Überwachungsbehörde im Hoheitsgebiet des

([21]) Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Jahresabschluss, den konsolidierten Abschluss und damit verbundene Berichte von Unternehmen bestimmter Rechtsformen und zur Änderung der Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinien 78/660/EWG und 83/349/EWG des Rates (ABl. L 182 vom 29.6.2013, S. 19).

betreffenden Drittlands ausübt, und keine Einwände dagegen erhoben haben. Um jedoch eine effiziente Umsetzung zu gewährleisten, müssen diese Befugnisse unbeschadet der jeweiligen Zuständigkeiten der Organe der Union bzw. der Mitgliedstaaten beim Abschluss von Vereinbarungen über die Verwaltungszusammenarbeit mit den einschlägigen Behörden des betreffenden Drittlands darin vollständig verankert werden. Diese Verordnung sollte es den ESA daher ermöglichen, mit den einschlägigen Behörden von Drittländern Vereinbarungen über die Verwaltungszusammenarbeit zu schließen, die keine anderweitigen rechtlichen Verpflichtungen gegenüber der Union und ihren Mitgliedstaaten begründen sollten.

(84) Um die Kommunikation mit der federführenden Überwachungsbehörde zu erleichtern und eine angemessene Vertretung sicherzustellen, sollten kritische IKT-Drittdienstleister, die Teil einer Gruppe sind, eine juristische Person als ihre Koordinierungsstelle benennen.

(85) Der Überwachungsrahmen sollte die Befugnis der Mitgliedstaaten unberührt lassen, eigene Aufsichts- oder Überwachungsmissionen in Bezug auf IKT-Drittdienstleister durchzuführen, die im Rahmen dieser Verordnung zwar nicht als kritisch eingestuft werden, aber auf nationaler Ebene als wichtig angesehen werden.

(86) Um die mehrschichtige institutionelle Architektur im Bereich der Finanzdienstleistungen zu nutzen, sollte der Gemeinsame Ausschuss der ESA im Einklang mit seinen Aufgaben im Bereich Cybersicherheit weiterhin die sektorübergreifende Gesamtkoordinierung für alle Fragen im Zusammenhang mit IKT-Risiken gewährleisten. Er sollte dabei durch einen neuen Unterausschuss (Überwachungsforum) unterstützt werden, der sowohl Einzelentscheidungen, die sich an kritische IKT-Drittdienstleister richten, als auch die Herausgabe gemeinsamer Empfehlungen, insbesondere in Bezug auf das Benchmarking der Überwachungsprogramme kritischer IKT-Drittdienstleister und zur Ermittlung bewährter Verfahren zur Bewältigung von Problemen im Zusammenhang mit IKT-Konzentrationsrisiken, vorbereitet.

(87) Um sicherzustellen, dass kritische IKT-Drittdienstleister auf Unionsebene angemessen und wirksam überwacht werden, könnte nach dieser Verordnung jede der drei ESA als federführende Überwachungsbehörde benannt werden. Die Entscheidung darüber, welcher der drei ESA ein kritischer IKT-Drittdienstleister konkret zugewiesen wird, sollte anhand einer Bewertung dessen getroffen werden, welche Finanzunternehmen in den Finanzbranchen, für die die betreffende ESA zuständig ist, überwiegend tätig sind. Dieser Ansatz sollte zu einer ausgewogenen Aufteilung der Aufgaben und Zuständigkeiten zwischen den drei ESA bei der Wahrnehmung ihrer Überwachungsfunktionen führen und die Humanressourcen und das technische Fachwissen, über die jede der drei ESA verfügen, bestmöglich nutzen.

(88) Federführende Überwachungsbehörden sollten mit den erforderlichen Befugnissen ausgestattet werden, Untersuchungen sowie Inspektionen vor Ort und von außerhalb bei kritischen IKT-Drittdienstleistern in deren Räumlichkeiten und an deren Standorten durchzuführen und vollständige und aktuelle Informationen zu erhalten. Diese Befugnisse sollten es der federführenden Überwachungsbehörde ermöglichen, Art, Ausmaß und Auswirkungen des IKT-Drittparteienrisikos für die Finanzunternehmen und letztlich für das Finanzsystem der Union, wahrheitsgetreu erfassen zu können. Die Übertragung der federführenden Überwachung auf die ESA ist eine Voraussetzung dafür, die systemische Dimension des IKT-Risikos im Finanzwesen zu verstehen und zu berücksichtigen. Der Einfluss kritischer IKT-Drittdienstleister auf den Finanzsektor der Union und die potenziellen Probleme, die durch das damit verbundene IKT-Konzentrationsrisiko verursacht werden, erfordern einen kollektiven Ansatz auf Unionsebene. Die gleichzeitige Durchführung mehrfacher Audits und Wahrnehmung von Zugangsrechten, die zahlreiche zuständige Behörden gesondert unter geringer oder keinerlei Abstimmung vornehmen, würden die Finanzaufsichtsbehörden daran hindern, sich einen vollständigen und umfassenden Überblick über das IKT-Drittparteienrisiko in der Union zu verschaffen und zudem gleichzeitig Redundanz, Belastungen und Komplexität für kritische IKT-Drittdienstleister mit sich bringen, wenn sie mit einer Vielzahl von Überwachungs- und Inspektionsanfragen konfrontiert sind.

(89) Aufgrund der erheblichen Auswirkungen, die mit der Einstufung als kritischer IKT-Drittdienstleister verbunden sind, sollte mit dieser Verordnung sichergestellt werden, dass die Rechte kritischer IKT-Drittdienstleister während der Umsetzung des Überwachungsrahmens gewahrt werden. Bevor sie als kritisch eingestuft werden, sollten diese Dienstleister beispielsweise berechtigt sein, der federführenden Überwachungsbehörde eine mit Gründen versehene Erklärung vorzulegen, die alle für die Beurteilung ihrer Einstufung relevanten Informationen enthält. Da die federführende Überwachungsbehörde befugt sein sollte, Empfehlungen zu IKT-Risiken und diesbezüglich geeigneten Abhilfemaßnahmen herauszugeben, was auch die Befugnis einschließt, bestimmte vertragliche Vereinbarungen, die letztlich die Stabilität des Finanzunternehmens oder des Finanzsystems beeinträchtigen, abzulehnen, sollte kritischen IKT-Drittdienstleistern ebenfalls die Möglichkeit eingeräumt werden, vor der Fertigstellung dieser Empfehlungen darzulegen, wie sich die darin aufgezeigten Lösungen voraussichtlich auf

Kunden auswirken werden, bei denen es sich um nicht in den Geltungsbereich dieser Verordnung fallende Unternehmen handelt, sowie Lösungen zur Risikominderung aufzuzeigen. Kritische IKT-Drittdienstleister, die den Empfehlungen nicht zustimmen, sollten eine begründete Erklärung über ihre Absicht, die Empfehlung nicht zu billigen, abgeben. Wird eine solche begründete Erklärung nicht abgegeben oder als unzureichend erachtet, sollte die federführende Überwachungsbehörde eine Mitteilung veröffentlichen, in der die strittige Angelegenheit kurz dargelegt wird.

(90) Die zuständigen Behörden sollten die Aufgabe, die inhaltliche Einhaltung der von der federführenden Überwachungsbehörde herausgegebenen Empfehlungen zu überprüfen, im Rahmen ihrer Tätigkeiten zur Beaufsichtigung von Finanzunternehmen gebührend wahrnehmen. Die zuständigen Behörden sollten Finanzunternehmen dazu verpflichten können, zusätzliche Maßnahmen zu ergreifen, um den in den Empfehlungen der federführenden Überwachungsbehörde ermittelten Risiken zu begegnen, und sollten zu gegebener Zeit entsprechende Mitteilungen herausgeben. Richtet die federführende Überwachungsbehörde Empfehlungen an kritische IKT-Drittdienstleister, die gemäß der Richtlinie (EU) 2022/2555 beaufsichtigt werden, so sollten die zuständigen Behörden auf freiwilliger Basis und vor dem Erlass zusätzlicher Maßnahmen die gemäß der genannten Richtlinie zuständigen Behörden konsultieren können, um einen koordinierten Ansatz in Bezug auf die betreffenden kritischen IKT-Drittdienstleister zu erleichtern.

(91) Die Ausübung der Überwachung sollte sich an drei Handlungsgrundsätzen orientieren, um Folgendes sicherzustellen: a) eine enge Koordinierung zwischen den ESA bei ihren Aufgaben als federführende Überwachungsbehörde mithilfe eines gemeinsamen Überwachungsnetzes (JON — Joint Oversight Network), b) die Kohärenz mit dem durch die Richtlinie (EU) 2022/2555 geschaffenen Rahmen (über eine freiwillige Konsultation der Einrichtungen, die in den Geltungsbereich der genannten Richtlinie fallen, um Doppelarbeit bei an kritische IKT-Drittdienstleister gerichteten Maßnahmen zu vermeiden) und c) eine Sorgfaltspflicht, wonach das potenzielle Risiko einer Störung der von kritischen IKT-Drittdienstleistern bereitgestellten Dienste für Kunden, bei denen es sich um nicht in den Geltungsbereich dieser Verordnung fallende Unternehmen handelt, zu minimieren ist.

(92) Der Überwachungsrahmen sollte nicht die Anforderung an Finanzunternehmen ersetzen, die Risiken, die die Nutzung von IKT-Drittdienstleistern mit sich bringt, selbst zu managen und sollte weder in irgendeiner Form noch für irgendeinen Aspekt an deren Stelle treten; dies schließt auch die Verpflichtung ein, die laufende Überwachung der mit kritischen IKT-Drittdienstleistern geschlossenen vertraglichen Vereinbarungen aufrechtzuerhalten. Ebenso sollte der Überwachungsrahmen die volle Verantwortung der Finanzunternehmen für die Einhaltung und Erfüllung aller Verpflichtungen gemäß dieser Verordnung und dem einschlägigen Finanzdienstleistungsrecht unberührt lassen.

(93) Um Doppelarbeit und Überschneidungen zu vermeiden, sollten die zuständigen Behörden davon absehen, im Alleingang Maßnahmen zur Überwachung des von kritischen IKT-Drittdienstleistern ausgehenden Risikos zu ergreifen, und sollten sich diesbezüglich auf die einschlägige Bewertung der federführenden Überwachungsbehörde stützen. Sämtliche Maßnahmen sollten in jedem Fall zuvor mit der federführenden Überwachungsbehörde im Rahmen der Ausübung ihrer Aufgaben innerhalb des Überwachungsrahmens koordiniert und vereinbart werden.

(94) Um auf internationaler Ebene die Konvergenz in Bezug auf bewährte Verfahren zu fördern, die für die Überprüfung und Überwachung des Managements von IKT-Drittdienstleistern ausgehender digitaler Risiken zu nutzen sind, sollten die ESA aufgefordert werden, Kooperationsvereinbarungen mit den zuständigen Aufsichts- und Regulierungsbehörden in Drittländern zu schließen.

(95) Um die speziellen Qualifikationen, die technischen Kompetenzen und das Fachwissen des auf operationelle und IKT-Risiken spezialisierten Personals innerhalb der zuständigen Behörden, der drei ESA und — auf freiwilliger Basis — der gemäß der Richtlinie (EU) 2022/2555 zuständigen Behörden zu nutzen, sollte die federführende Überwachungsbehörde auf nationale Aufsichtsfähigkeiten und das entsprechende Fachwissen zurückgreifen und für jeden einzelnen kritischen IKT-Drittdienstleister spezielle Untersuchungsteams einrichten und multidisziplinäre Teams zusammenlegen, um sowohl die Vorbereitung als auch die tatsächliche Wahrnehmung von Überwachungstätigkeiten zu unterstützen, einschließlich allgemeiner Untersuchungen und Inspektionen kritischer IKT-Drittdienstleister sowie jeglicher erforderlichen Folgemaßnahmen.

(96) Während die Kosten, die sich aus den Überwachungsaufgaben ergeben, vollständig aus Gebühren finanziert würden, die von kritischen IKT-Drittdienstleistern erhoben werden, dürften den ESA hingegen vor Beginn des Überwachungsrahmens Kosten für die Einführung spezieller IKT-Systeme zur Unterstützung der anstehenden Überwachung entstehen, da im Vorfeld spezielle IKT-Systeme entwickelt und eingeführt werden müssten. Diese Verordnung sieht daher ein hybrides Finanzierungsmodell vor, bei dem der Überwachungsrahmen als solcher vollständig gebührenfinanziert wäre, während die Entwicklung der IKT-Systeme der ESA aus Beiträgen der Union und der zuständigen nationalen Behörden finanziert würde.

(97) Zuständige Behörden sollten über alle erforderlichen Aufsichts-, Untersuchungs- und Sanktionsbefugnisse verfügen, um die angemessene Wahrnehmung ihrer Aufgaben im Rahmen dieser Verordnung sicherzustellen. Sie sollten grundsätzlich die von ihnen verhängten Verwaltungssanktionen öffentlich bekannt machen. Da Finanzunternehmen und kritische IKT-Drittdienstleister in unterschiedlichen Mitgliedstaaten ansässig sein und der Aufsicht unterschiedlicher zuständiger Behörden unterliegen können, sollte die Anwendung dieser Verordnung zum einen durch die enge Zusammenarbeit zwischen den jeweils zuständigen Behörden, einschließlich der EZB bei der Wahrnehmung der ihr durch die Verordnung (EU) Nr. 1024/2013 übertragenen besonderen Aufgaben, erleichtert werden sowie zum anderen durch die Abstimmung mit den ESA im Wege des gegenseitigen Informationsaustauschs und der Erbringung von Amtshilfe in den einschlägigen Aufsichtsbelangen.

(98) Um die Kriterien für die Einstufung von IKT-Drittdienstleistern als kritisch weiter zu quantifizieren und zu präzisieren und um Überwachungsgebühren zu harmonisieren, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zur Ergänzung dieser Verordnung in Bezug auf Folgendes zu erlassen: die weitere Präzisierung der systemischen Auswirkungen, die ein Ausfall eines Dienstes oder ein operativer Ausfall eines IKT-Drittdienstleisters auf die Finanzunternehmen haben könnte, für die er IKT-Dienstleistungen bereitstellt; die Anzahl global systemrelevanter Institute (G-SRI) oder anderer systemrelevanter Institute (A-SRI), die auf den betreffenden IKT-Drittdienstleister angewiesen sind; die Zahl der IKT-Drittdienstleister, die auf einem bestimmten Markt tätig sind; die Kosten für die Migration von Daten und IKT-Arbeitslasten zu anderen IKT-Drittdienstleistern; sowie den Betrag der Überwachungsgebühren und die damit verbundene Zahlungsweise. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung ([22]) niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, sollten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten erhalten, und ihre Sachverständigen sollten systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission haben, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(99) Die kohärente Harmonisierung der in dieser Verordnung festgelegten Anforderungen sollte durch technische Regulierungsstandards gewährleistet werden. In ihrer Funktion als Stellen, die über hochspezialisierte Fachkräfte verfügen, sollten die ESA Entwürfe technischer Regulierungsstandards ausarbeiten, die keine politischen Entscheidungen erfordern, und sie der Kommission vorlegen. In den Bereichen IKT-Risikomanagement, Meldung schwerwiegender IKT-bezogener Vorfälle, Tests sowie in Bezug auf Schlüsselanforderungen für eine solide Überwachung des IKT-Drittparteienrisikos sollten technische Regulierungsstandards entwickelt werden. Die Kommission und die ESA sollten sicherstellen, dass diese Standards und Anforderungen von allen Finanzunternehmen auf eine Weise angewandt werden können, die ihrer Größe und ihrem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte angemessen ist. Der Kommission sollte die Befugnis übertragen werden, diese technischen Regulierungsstandards mittels delegierter Rechtsakten gemäß Artikel 290 AEUV und im Einklang mit den Artikeln 10 und 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu erlassen.

(100) Um die Vergleichbarkeit der Meldungen über schwerwiegende IKT-bezogene Vorfälle und schwerwiegende zahlungsbezogene Betriebs- oder Sicherheitsvorfälle zu erleichtern sowie um für Transparenz in Bezug auf vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen von Drittdienstleistern zu sorgen, sollten die ESA Entwürfe technischer Durchführungsstandards erarbeiten, mit denen standardisierte Vorlagen, Formulare und Verfahren für Finanzunternehmen zur Meldung schwerwiegender IKT-bezogener Vorfälle und schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle sowie standardisierte Vorlagen für das Informationsregister festgelegt werden. Bei der Ausarbeitung dieser Standards sollten die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte berücksichtigen. Der Kommission sollte die Befugnis übertragen werden, diese technischen Durchführungsstandards mittels Durchführungsrechtsakten gemäß Artikel 291 AEUV und im Einklang mit Artikel 15 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu erlassen.

([22]) ABl. L 123 vom 12.5.2016, S. 1.

(101) Da weitere Anforderungen bereits durch delegierte Rechtsakte und Durchführungsrechtsakte auf der Grundlage technischer Regulierungs- und Durchführungsstandards in den Verordnungen (EG) Nr. 1060/2009 ([23]), (EU) Nr. 648/2012 ([24]), (EU) Nr. 600/2014 ([25]) bzw. (EU) Nr. 909/2014 ([26]) des Europäischen Parlaments und des Rates festgelegt wurden, ist es angezeigt, die ESA entweder einzeln oder gemeinsam über den Gemeinsamen Ausschuss zu beauftragen, der Kommission technische Regulierungs- und Durchführungsstandards für den Erlass von delegierten Rechtsakten und Durchführungsrechtsakten zur Übernahme und Aktualisierung bestehender IKT-Risikomanagementvorschriften vorzulegen.

(102) Da die vorliegende Verordnung in Verbindung mit der Richtlinie (EU) 2022/2556 des Europäischen Parlaments und des Rates ([27]) eine Konsolidierung der Bestimmungen über IKT-Risikomanagement mit sich bringt, die sich über mehrere Verordnungen und Richtlinien des Besitzstands der Union im Bereich der Finanzdienstleistungen erstrecken, einschließlich der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014 und der Verordnung (EU) 2016/1011 ([28]) des Europäischen Parlaments und des Rates, sollten diese Verordnungen zur Gewährleistung vollständiger Übereinstimmung geändert werden, damit klargestellt ist, dass die geltenden Bestimmungen über IKT-Risiken in der vorliegenden Verordnung verankert sind.

(103) Der Geltungsbereich der einschlägigen Artikel über operationelle Risiken, auf deren Grundlage durch Befugnisübertragungen gemäß den Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 (EU) Nr. 909/2014 und (EU) 2016/1011 der Erlass von delegierten Rechtsakten und Durchführungsrechtsakten ermöglicht wurde, sollte folglich eingeschränkt werden, damit alle Bestimmungen, die Aspekte der digitalen operationalen Resilienz betreffen und heute Teil der genannten Verordnungen sind, in die vorliegende Verordnung übernommen werden können.

(104) Das potenzielle systemische Cyberrisiko, das mit der Nutzung von IKT-Infrastrukturen verbunden ist, die den Betrieb von Zahlungssystemen und die Erbringung von Zahlungsabwicklungstätigkeiten ermöglichen, sollte auf Unionsebene durch harmonisierte Vorschriften für die digitale Resilienz angemessen angegangen werden. Zu diesem Zweck sollte die Kommission rasch prüfen, ob der Geltungsbereich der vorliegenden Verordnung überprüft werden muss, und diese Überprüfung zugleich an die Ergebnisse der in der Richtlinie (EU) 2015/2366 vorgesehenen umfassenden Überprüfung anpassen. Zahlreiche Großangriffe in den letzten zehn Jahren haben gezeigt, inwiefern Zahlungssysteme Cyberbedrohungen ausgesetzt sind. Da sie im Mittelpunkt der Zahlungsdienstleistungskette stehen und starke Verflechtungen mit dem gesamten Finanzsystem aufweisen, sind Zahlungssysteme und Zahlungsabwicklungstätigkeiten nunmehr zu einem maßgeblichen Faktor für das Funktionieren der Finanzmärkte der Union geworden. Cyberangriffe auf diese Systeme können zu schwerwiegenden Betriebsstörungen führen, die sich direkt auf wirtschaftliche Schlüsselfunktionen wie die Erleichterung von Zahlungen auswirken und zugleich indirekt Konsequenzen für die damit verbundenen wirtschaftlichen Prozesse haben. Bis zur Einführung eines harmonisierten Systems und der Beaufsichtigung der Betreiber von Zahlungssystemen und Zahlungsabwicklungsunternehmen auf Unionsebene können sich die Mitgliedstaaten zur Anwendung ähnlicher Marktpraktiken an den mit dieser Verordnung festgelegten Anforderungen an die digitale operationale Resilienz orientieren, wenn sie für Betreiber von Zahlungssystemen und Zahlungsabwicklungsunternehmen, die in ihrem jeweiligen Hoheitsgebiet der Aufsicht unterliegen, diesbezügliche Vorschriften anwenden.

([23]) Verordnung (EG) Nr. 1060/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 über Ratingagenturen (ABl. L 302 vom 17.11.2009, S. 1).

([24]) 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).

([25]) 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).

([26]) 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).

([27]) Richtlinie (EU) 2022/2556 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 zur Änderung der Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 und (EU) 2016/2341 hinsichtlich der digitalen operationalen Resilienz im Finanzsektor (siehe Seite 153 dieses Amtsblatts).

([28]) Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über Indizes, die bei Finanzinstrumenten und Finanzkontrakten als Referenzwert oder zur Messung der Wertentwicklung eines Investmentfonds verwendet werden, und zur Änderung der Richtlinien 2008/48/EG und 2014/17/EU sowie der Verordnung (EU) Nr. 596/2014 (ABl. L 171 vom 29.6.2016, S. 1).

(105) Da das Ziel dieser Verordnung, nämlich die Erreichung eines hohen Niveaus an digitaler operationaler Resilienz in beaufsichtigten Finanzunternehmen, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, weil es der Harmonisierung einiger unterschiedlicher Vorschriften im Unionsrecht und im nationalen Recht bedarf, sondern vielmehr wegen seines Umfangs und seiner Wirkungen auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

(106) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([29]) konsultiert und hat am 10. Mai 2021 eine Stellungnahme abgegeben ([30]) —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand

(1) Um ein hohes gemeinsames Niveau an digitaler operationaler Resilienz zu erreichen, werden in dieser Verordnung einheitliche Anforderungen für die Sicherheit von Netzwerk- und Informationssystemen, die die Geschäftsprozesse von Finanzunternehmen unterstützen, wie folgt festgelegt:

a) auf Finanzunternehmen anwendbare Anforderungen in Bezug auf:

   i) Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT);

   ii) Meldung schwerwiegender IKT-bezogener Vorfälle und — auf freiwilliger Basis — erheblicher Cyberbedrohungen an die zuständigen Behörden;

   iii) Meldung schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle durch in Artikel 2 Absatz 1 Buchstaben a bis d aufgeführte Finanzunternehmen an die zuständigen Behörden;

   iv) Tests der digitalen operationalen Resilienz;

   v) Austausch von Informationen und Erkenntnissen in Bezug auf Cyberbedrohungen und Schwachstellen;

   vi) Maßnahmen für das solide Management des IKT-Drittparteienrisikos;

b) Anforderungen in Bezug auf vertragliche Vereinbarungen zwischen IKT-Drittdienstleistern und Finanzunternehmen;

c) Vorschriften über die Einrichtung und Ausführung des Überwachungsrahmens für kritische IKT-Drittdienstleister bei der Erbringung von Dienstleistungen für Finanzunternehmen;

d) Vorschriften über die Zusammenarbeit zwischen zuständigen Behörden und Vorschriften über die Beaufsichtigung und Durchsetzung aller von dieser Verordnung erfassten Sachverhalte durch zuständige Behörden.

(2) In Bezug auf Finanzunternehmen, die gemäß den nationalen Vorschriften zur Umsetzung von Artikel 3 der Richtlinie (EU) 2022/2555 als wesentliche oder wichtige Unternehmen ermittelt wurden, gilt diese Verordnung für die Zwecke von Artikel 4 der genannten Richtlinie als sektorspezifischer Rechtsakt der Union.

(3) Diese Verordnung lässt die Zuständigkeiten der Mitgliedstaaten für grundlegende Funktionen des Staates in Bezug auf die öffentliche Sicherheit, die Landesverteidigung und die nationale Sicherheit im Einklang mit dem Unionsrecht unberührt.

([29]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

([30]) ABl. C 229 vom 15.6.2021, S. 16.

Artikel 2

Geltungsbereich

(1) Unbeschadet der Absätze 3 und 4 gilt diese Verordnung für folgende Unternehmen:

a) Kreditinstitute,

b) Zahlungsinstitute, einschließlich gemäß der Richtlinie (EU) 2015/2366 ausgenommene Zahlungsinstitute,

c) Kontoinformationsdienstleister,

d) E-Geld-Institute, einschließlich gemäß der Richtlinie 2009/110/EG ausgenommene E-Geld-Institute,

e) Wertpapierfirmen,

f) Anbieter von Krypto-Dienstleistungen, die gemäß einer Verordnung des Europäischen Parlaments und des Rates über Märkte von Krypto-Werten und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 (im Folgenden „Verordnung über Märkte von Krypto-Werten“) zugelassen sind, und Emittenten wertreferenzierter Token,

g) Zentralverwahrer,

h) zentrale Gegenparteien,

i) Handelsplätze,

j) Transaktionsregister,

k) Verwalter alternativer Investmentfonds,

l) Verwaltungsgesellschaften,

m) Datenbereitstellungsdienste,

n) Versicherungs- und Rückversicherungsunternehmen,

o) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit,

p) Einrichtungen der betrieblichen Altersversorgung,

q) Ratingagenturen,

r) Administratoren kritischer Referenzwerte,

s) Schwarmfinanzierungsdienstleister,

t) Verbriefungsregister,

u) IKT-Drittdienstleister.

(2) Für die Zwecke dieser Verordnung werden die in Absatz 1 Buchstaben a bis t genannten Unternehmen zusammen als „Finanzunternehmen“ bezeichnet.

(3) Diese Verordnung gilt nicht für:

a) Verwalter alternativer Investmentfonds im Sinne von Artikel 3 Absatz 2 der Richtlinie 2011/61/EU;

b) Versicherungs- und Rückversicherungsunternehmen im Sinne von Artikel 4 der Richtlinie 2009/138/EG;

c) Einrichtungen der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt weniger als 15 Versorgungsanwärtern betreiben;

d) gemäß den Artikeln 2 und 3 der Richtlinie 2014/65/EU ausgenommene natürliche oder juristische Personen;

e) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, bei denen es sich um Kleinstunternehmen oder kleine oder mittlere Unternehmen handelt;

f) Postgiroämter im Sinne von Artikel 2 Absatz 5 Nummer 3 der Richtlinie 2013/36/EU.

(4) Die Mitgliedstaaten können die in Artikel 2 Absatz 5 Nummern 4 bis 23 der Richtlinie 2013/36/EU aufgeführten Stellen, die sich in ihrem jeweiligen Hoheitsgebiet befinden, vom Geltungsbereich dieser Verordnung ausnehmen. Macht ein Mitgliedstaat von dieser Möglichkeit Gebrauch, so setzt er die Kommission hiervon sowie von allen nachfolgenden Änderungen in Kenntnis. Die Kommission macht diese Informationen auf ihrer Website oder auf andere leicht zugängliche Weise öffentlich zugänglich.

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck:

1. „digitale operationale Resilienz“ die Fähigkeit eines Finanzunternehmens, seine operative Integrität und Betriebszuverlässigkeit aufzubauen, zu gewährleisten und zu überprüfen, indem es entweder direkt oder indirekt durch Nutzung der von IKT-Drittdienstleistern bereitgestellten Dienste das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die Sicherheit der Netzwerk- und Informationssysteme zu gewährleisten, die von einem Finanzunternehmen genutzt werden und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität, einschließlich bei Störungen, unterstützen;

2. „Netzwerk- und Informationssystem“ ein Netz- und Informationssystem im Sinne von Artikel 6 Nummer 1 der Richtlinie (EU) 2022/2555;

3. „IKT-Altsystem“ ein IKT-System, das das Ende seines Lebenszyklus (Ende seiner Lebensdauer) erreicht hat, aus technologischen oder wirtschaftlichen Gründen nicht für Upgrades oder Fehlerbehebungen in Frage kommt oder nicht mehr von seinem Anbieter oder einem IKT-Drittdienstleister unterstützt wird, das allerdings weiterhin genutzt wird und die Funktionen des Finanzunternehmens unterstützt;

4. „Sicherheit von Netzwerk- und Informationssystemen“ die Sicherheit von Netz- und Informationssystemen im Sinne von Artikel 6 Nummer 2 der Richtlinie (EU) 2022/2555;

5. „IKT-Risiko“ jeden vernünftigerweise identifizierbaren Umstand im Zusammenhang mit der Nutzung von Netzwerk- und Informationssystemen, der bei Eintritt durch die damit einhergehenden nachteiligen Auswirkungen im digitalen oder physischen Umfeld die Sicherheit der Netzwerk- und Informationssysteme, jeglicher technologieabhängiger Instrumente oder Prozesse, von Geschäften und Prozessen oder der Bereitstellung von Diensten beeinträchtigen kann.

6. „Informationsasset“ eine Sammlung materieller oder immaterieller Informationen, die geschützt werden sollten;

7. „IKT-Asset“ eine Software oder Hardware in den Netzwerk- und Informationssystemen, die das Finanzunternehmen nutzt;

8. „IKT-bezogener Vorfall“ ein von dem Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, das bzw. die die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigt und nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Finanzunternehmen erbrachten Dienstleistungen hat;

9. „zahlungsbezogener Betriebs- oder Sicherheitsvorfall“ ein von den in Artikel 2 Absatz 1 Buchstaben a bis d aufgeführten Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, unabhängig davon, ob es sich um IKT-bezogene Vorfälle handelt oder nicht, das bzw. die nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit zahlungsbezogener Daten oder auf die vom Finanzunternehmen bereitgestellten zahlungsbezogenen Dienste hat;

10. „schwerwiegender IKT-bezogener Vorfall“ einen IKT-Vorfall, der umfassende nachteilige Auswirkungen auf die Netzwerk- und Informationssysteme hat, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen;

11. „schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfall“ einen zahlungsbezogenen Betriebs- oder Sicherheitsvorfall, der umfassende nachteilige Auswirkungen auf die bereitgestellten zahlungsbezogenen Dienste hat;

12. „Cyberbedrohung“ eine Cyberbedrohung im Sinne von Artikel 2 Nummer 8 der Verordnung (EU) 2019/881;

13. „erhebliche Cyberbedrohung“ eine Cyberbedrohung, deren technische Merkmale darauf hindeuten, dass sie das Potenzial haben könnte, einen schwerwiegenden IKT-bezogenen Vorfall oder einen schwerwiegenden zahlungsbezogenen Betriebs- oder Sicherheitsvorfall zu verursachen;

14. „Cyberangriff“ einen böswilligen IKT-bezogenen Vorfall, der auf den Versuch eines Angreifers zurückgeht, einen Vermögenswert zu zerstören, freizulegen, zu verändern, zu deaktivieren, zu entwenden oder auf unberechtigte Weise auf diesen Vermögenswert zuzugreifen oder ihn auf unberechtigte Weise zu nutzen;

15. „Bedrohungsanalyse“ Informationen, die aggregiert, umgewandelt, analysiert, ausgewertet oder erweitert wurden, um den notwendigen Kontext für die Entscheidungsfindung zu schaffen und ein relevantes und ausreichendes Verständnis für die Abmilderung der Auswirkungen eines IKT-bezogenen Vorfalls oder einer Cyberbedrohung zu ermöglichen, einschließlich der technischen Einzelheiten eines Cyberangriffs, der für den Angriff verantwortlichen Personen und ihres Modus Operandi und ihrer Beweggründe;

16. „Schwachstelle“ eine Schwachstelle, Empfindlichkeit oder Fehlfunktion eines Vermögenswerts, eines Systems, eines Prozesses oder einer Kontrolle, die ausgenutzt werden kann;

17. „bedrohungsorientierte Penetrationstests (TLPT — Threat-Led Penetration Testing)“ einen Rahmen, der Taktik, Techniken und Verfahren realer Angreifer, die als echte Cyberbedrohung empfunden werden, nachbildet und einen kontrollierten, maßgeschneiderten, erkenntnisgestützten (Red-Team-) Test der kritischen Live-Produktionssysteme des Finanzunternehmens ermöglicht;

18. „IKT-Drittparteienrisiko“ ein IKT-bezogenes Risiko, das für ein Finanzunternehmen im Zusammenhang mit dessen Nutzung von IKT-Dienstleistungen entstehen kann, die von IKT-Drittdienstleistern oder deren Unterauftragnehmern, einschließlich über Vereinbarungen zur Auslagerung, bereitgestellt werden;

19. „IKT-Drittdienstleister“ ein Unternehmen, das IKT-Dienstleistungen bereitstellt;

20. „gruppeninterner IKT-Dienstleister“ ein Unternehmen, das Teil einer Finanzgruppe ist und überwiegend IKT-Dienstleistungen für Finanzunternehmen derselben Gruppe oder für Finanzunternehmen, die demselben institutsbezogenen Sicherungssystem angehören, bereitstellt, einschließlich deren Mutterunternehmen, Tochterunternehmen und Zweigniederlassungen oder anderer Unternehmen, die in gemeinsamem Eigentum oder unter gemeinsamer Kontrolle stehen;

21. „IKT-Dienstleistungen“ digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste;

22. „kritische oder wichtige Funktion“ eine Funktion, deren Ausfall die finanzielle Leistungsfähigkeit eines Finanzunternehmens oder die Solidität oder Fortführung seiner Geschäftstätigkeiten und Dienstleistungen erheblich beeinträchtigen würde oder deren unterbrochene, fehlerhafte oder unterbliebene Leistung die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht erheblich beeinträchtigen würde;

23. „kritischer IKT-Drittdienstleister“ einen IKT-Drittdienstleister, der gemäß Artikel 31 als kritisch eingestuft wurde;

24. „IKT-Drittdienstleister mit Sitz in einem Drittland“ einen IKT-Drittdienstleister, bei dem es sich um eine in einem Drittland niedergelassene juristische Person handelt, die mit einem Finanzunternehmen eine vertragliche Vereinbarung über die Bereitstellung von IKT-Dienstleistungen geschlossen hat;

25. „Tochterunternehmen“ ein Tochterunternehmen im Sinne von Artikel 2 Nummer 10 und Artikel 22 der Richtlinie 2013/34/EU;

26. „Gruppe“ eine Gruppe im Sinne von Artikel 2 Nummer 11 der Richtlinie 2013/34/EU;

27. „Mutterunternehmen“ ein Mutterunternehmen im Sinne von Artikel 2 Nummer 9 und Artikel 22 der Richtlinie 2013/34/EU;

28. „IKT-Unterauftragnehmer mit Sitz in einem Drittland“ einen IKT-Unterauftragnehmer, bei dem es sich um eine in einem Drittland niedergelassene juristische Person handelt, die mit einem IKT-Drittdienstleister oder einem IKT-Drittdienstleister mit Sitz in einem Drittland eine vertragliche Vereinbarung geschlossen hat;

29. „IKT-Konzentrationsrisiko“ die Exposition gegenüber einzelnen oder mehreren verbundenen kritischen IKT-Drittdienstleistern, die zu einer gewissen Abhängigkeit von diesen Dienstleistern führt, sodass die Nichtverfügbarkeit, der Ausfall oder sonstige Defizite dieser Dienstleister die Fähigkeit eines Finanzunternehmens gefährden könnten, kritische oder wichtige Funktionen zu erfüllen, oder bei dem Finanzunternehmen andere Formen nachteiliger Auswirkungen, einschließlich großer Verluste, herbeiführen oder die finanzielle Stabilität der Union insgesamt gefährden könnten;

30. „Leitungsorgan“ ein Leitungsorgan im Sinne von Artikel 4 Absatz 1 Nummer 36 der Richtlinie 2014/65/EU, von Artikel 3 Absatz 1 Nummer 7 der Richtlinie 2013/36/EU, von Artikel 2 Absatz 1 Buchstabe s der Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates ([31]), von Artikel 2 Absatz 1 Nummer 45 der Verordnung (EU) Nr. 909/2014, von Artikel 3 Absatz 1 Nummer 20 der Verordnung (EU) 2016/1011 sowie im Sinne der einschlägigen Vorschrift der Verordnung über Märkte von Krypto-Werten oder die entsprechenden Personen, die das Unternehmen tatsächlich leiten oder im Einklang mit dem einschlägigen Unionsrecht oder nationalen Recht Schlüsselfunktionen wahrnehmen;

31. „Kreditinstitut“ ein Kreditinstitut im Sinne von Artikel 4 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates ([32]);

32. „nach der Richtlinie 2013/36/EU ausgenommenes Institut“ eine in Artikel 2 Absatz 5 Nummern 4 bis 23 der Richtlinie 2013/36/EU aufgeführte Einrichtung;

33. „Wertpapierfirma“ eine Wertpapierfirma im Sinne von Artikel 4 Absatz 1 Nummer 1 der Richtlinie 2014/65/EU;

34. „kleine und nicht verflochtene Wertpapierfirma“ eine Wertpapierfirma, die die in Artikel 12 Absatz 1 der Verordnung (EU) 2019/2033 des Europäischen Parlaments und des Rates ([33]) genannten Bedingungen erfüllt;

35. „Zahlungsinstitut“ ein Zahlungsinstitut im Sinne von Artikel 4 Nummer 4 der Richtlinie (EU) 2015/2366;

36. „nach der Richtlinie (EU) 2015/2366 ausgenommenes Zahlungsinstitut“ ein Zahlungsinstitut, für das eine Ausnahme nach Artikel 32 Absatz 1 der Richtlinie (EU) 2015/2366 gilt;

37. „Kontoinformationsdienstleister“ einen Kontoinformationsdienstleister im Sinne von Artikel 33 Absatz 1 der Richtlinie (EU) 2015/2366;

38. „E-Geld-Institut“ ein E-Geld-Institut im Sinne von Artikel 2 Nummer 1 der Richtlinie 2009/110/EG;

39. „nach der Richtlinie 2009/110/EG ausgenommenes E-Geld-Institut“ ein E-Geld-Institut, für das eine Ausnahme nach Artikel 9 Absatz 1 der Richtlinie 2009/110/EG gilt;

40. „zentrale Gegenpartei“ eine zentrale Gegenpartei im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) Nr. 648/2012;

41. „Transaktionsregister“ ein Transaktionsregister im Sinne von Artikel 2 Nummer 2 der Verordnung (EU) Nr. 648/2012;

42. „Zentralverwahrer“ ein Zentralverwahrer im Sinne von Artikel 2 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 909/2014;

43. „Handelsplatz“ einen Handelsplatz im Sinne von Artikel 4 Absatz 1 Nummer 24 der Richtlinie 2014/65/EU.

44. „Verwalter alternativer Investmentfonds“ einen Verwalter alternativer Investmentfonds im Sinne von Artikel 4 Absatz 1 Buchstabe b der Richtlinie 2011/61/EU;

45. „Verwaltungsgesellschaft“ eine Verwaltungsgesellschaft im Sinne von Artikel 2 Absatz 1 Buchstabe b der Richtlinie 2009/65/EG.

46. „Datenbereitstellungsdienst“ einen in Artikel 2 Absatz 1 Nummern 34 bis 36 der Verordnung (EU) Nr. 600/2014 genannten Datenbereitstellungsdienst im Sinne der genannten Verordnung;

47. „Versicherungsunternehmen“ ein Versicherungsunternehmen im Sinne von Artikel 13 Nummer 1 der Richtlinie 2009/138/EG;

48. „Rückversicherungsunternehmen“ ein Rückversicherungsunternehmen im Sinne von Artikel 13 Nummer 4 der Richtlinie 2009/138/EG;

([31]) Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 zur Koordinierung der Rechts- und Verwaltungsvorschriften betreffend bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (OGAW) (ABl. L 302 vom 17.11.2009, S. 32).

([32]) Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1).

([33]) Verordnung (EU) 2019/2033 des Europäischen Parlaments und des Rates vom 27. November 2019 über Aufsichtsanforderungen an Wertpapierfirmen und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 575/2013, (EU) Nr. 600/2014 und (EU) Nr. 806/2014 (ABl. L 314 vom 5.12.2019, S. 1).

49. „Versicherungsvermittler“ einen Versicherungsvermittler im Sinne von Artikel 2 Absatz 1 Nummer 3 der Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates ([34]);

50. „Versicherungsvermittler in Nebentätigkeit“ einen Versicherungsvermittler in Nebentätigkeit im Sinne von Artikel 2 Absatz 1 Nummer 4 der Richtlinie (EU) 2016/97;

51. „Rückversicherungsvermittler“ einen Rückversicherungsvermittler im Sinne von Artikel 2 Absatz 1 Nummer 5 der Richtlinie (EU) 2016/97;

52. „Einrichtung der betrieblichen Altersversorgung“ eine Einrichtung der betrieblichen Altersversorgung im Sinne von Artikel 6 Nummer 1 der Richtlinie (EU) 2016/2341;

53. „kleine Einrichtung der betrieblichen Altersversorgung“ eine Einrichtung der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt weniger als 100 Versorgungsanwärtern betreibt;

54. „Ratingagentur“ eine Ratingagentur im Sinne von Artikel 3 Absatz 1 Buchstabe b der Verordnung (EG) Nr. 1060/2009;

55. „Anbieter von Krypto-Dienstleistungen“ einen Anbieter von Krypto-Dienstleistungen im Sinne der einschlägigen Vorschrift der Verordnung über Märkte von Krypto-Werten;

56. „Emittent wertreferenzierter Token“ einen Emittenten „wertreferenzierter Token“ im Sinne der einschlägigen Vorschrift der Verordnung über Märkte von Krypto-Werten;

57. „Administrator kritischer Referenzwerte“ einen Administrator „kritischer Referenzwerte“ im Sinne von Artikel 3 Absatz 1 Nummer 25 der Verordnung (EU) 2016/1011;

58. „Schwarmfinanzierungsdienstleister“ einen Schwarmfinanzierungsdienstleister im Sinne von Artikel 2 Absatz 1 Buchstabe e der Verordnung (EU) 2020/1503 des Europäischen Parlaments und des Rates ([35]);

59. „Verbriefungsregister“ ein Verbriefungsregister im Sinne von Artikel 2 Nummer 23 der Verordnung (EU) 2017/2402 des Europäischen Parlaments und des Rates ([36]);

60. „Kleinstunternehmen“ ein Finanzunternehmen, bei dem es sich nicht um einen Handelsplatz, eine zentrale Gegenpartei, ein Transaktionsregister oder einen Zentralverwahrer handelt, das weniger als zehn Personen beschäftigt und dessen Jahresumsatz bzw. -bilanzsumme 2 Mio. EUR nicht überschreitet;

61. „federführende Überwachungsbehörde“ die gemäß Artikel 31 Absatz 1 Buchstabe b dieser Verordnung benannte Europäische Aufsichtsbehörde;

62. „Gemeinsamer Ausschuss“ den jeweils in Artikel 54 der Verordnung (EU) Nr. 1093/2010, der Verordnung (EU) Nr. 1094/2010 und der Verordnung (EU) Nr. 1095/2010 genannten Ausschuss;

63. „Kleinunternehmen“ ein Finanzunternehmen, das 10 oder mehr, aber weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. -bilanzsumme 2 Mio. EUR überschreitet, nicht jedoch 10 Mio. EUR;

64. „mittleres Unternehmen“ ein Finanzunternehmen, das kein Kleinunternehmen ist, das weniger als 250 Personen beschäftigt und dessen Jahresumsatz 50 Mio. EUR und/oder dessen Jahresbilanzsumme 43 Mio. EUR nicht überschreitet;

65. „staatliche Behörde“ jede staatliche Stelle oder sonstige Stelle der öffentlichen Verwaltung, einschließlich der nationalen Zentralbanken.

([34]) Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates vom 20. Januar 2016 über Versicherungsvertrieb (ABl. L 26 vom 2.2.2016, S. 19).

([35]) Verordnung (EU) 2020/1503 des Europäischen Parlaments und des Rates vom 7. Oktober 2020 über Europäische Schwarmfinanzierungsdienstleister für Unternehmen und zur Änderung der Verordnung (EU) 2017/1129 und der Richtlinie (EU) 2019/1937 (ABl. L 347 vom 20.10.2020, S. 1).

([36]) Verordnung (EU) 2017/2402 des Europäischen Parlaments und des Rates vom 12. Dezember 2017 zur Festlegung eines allgemeinen Rahmens für Verbriefungen und zur Schaffung eines spezifischen Rahmens für einfache, transparente und standardisierte Verbriefung und zur Änderung der Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU und der Verordnungen (EG) Nr. 1060/2009 und (EU) Nr. 648/2012 (ABl. L 347 vom 28.12.2017, S. 35).

Artikel 4

Grundsatz der Verhältnismäßigkeit

(1) Die Finanzunternehmen wenden die in Kapitel II festgelegten Vorschriften im Einklang mit dem Grundsatz der Verhältnismäßigkeit an, wobei ihrer Größe und ihrem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte Rechnung zu tragen ist.

(2) Darüber hinaus muss die Anwendung der Kapitel III und IV sowie des Kapitels V Abschnitt I durch die Finanzunternehmen in einem angemessenen Verhältnis zu ihrer Größe und ihrem Gesamtrisikoprofil sowie zu der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte stehen, wie dies in den einschlägigen Vorschriften jener Kapitel ausdrücklich vorgesehen ist.

(3) Bei der Überprüfung der Kohärenz des IKT-Risikomanagementrahmens auf der Grundlage der Berichte, die den zuständigen Behörden gemäß Artikel 6 Absatz 5 und Artikel 16 Absatz 2 auf Anfrage vorgelegt werden, prüfen die zuständigen Behörden die Anwendung des Grundsatzes der Verhältnismäßigkeit durch die Finanzunternehmen.

KAPITEL II

IKT-Risikomanagement

Abschnitt I

Artikel 5

Governance und Organisation

(1) Finanzunternehmen verfügen über einen internen Governance- und Kontrollrahmen, der im Einklang mit Artikel 6 Absatz 4 ein wirksames und umsichtiges Management von IKT-Risiken gewährleistet, um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen.

(2) Das Leitungsorgan des Finanzunternehmens definiert, genehmigt, überwacht und verantwortet die Umsetzung aller Vorkehrungen im Zusammenhang mit dem IKT-Risikomanagementrahmen nach Artikel 6 Absatz 1.

Für die Zwecke von Unterabsatz 1 gilt Folgendes:

a) Das Leitungsorgan trägt die letztendliche Verantwortung für das Management der IKT-Risiken des Finanzunternehmens;

b) das Leitungsorgan führt Leitlinien ein, die darauf abzielen, hohe Standards in Bezug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten aufrechtzuerhalten;

c) das Leitungsorgan legt klare Aufgaben und Verantwortlichkeiten für alle IKT-bezogenen Funktionen sowie angemessene Governance-Regelungen fest, um eine wirksame und rechtzeitige Kommunikation, Zusammenarbeit und Koordinierung zwischen diesen Funktionen zu gewährleisten;

d) das Leitungsorgan trägt die Gesamtverantwortung für die Festlegung und Genehmigung der Strategie für die digitale operationale Resilienz gemäß Artikel 6 Absatz 8, einschließlich der Festlegung der angemessenen Toleranzschwelle für das IKT-Risiko des Finanzunternehmens gemäß Artikel 6 Absatz 8 Buchstabe b;

e) das Leitungsorgan genehmigt, überwacht und überprüft regelmäßig die Umsetzung der in Artikel 11 Absatz 1 genannten IKT-Geschäftsfortführungsleitlinie und der in Artikel 11 Absatz 3 genannten IKT-Reaktions- und Wiederherstellungspläne, die als eigenständige spezielle Leitlinie, die integraler Bestandteil der allgemeinen Geschäftsfortführungsleitlinie des Finanzunternehmens und seines Reaktions- und Wiederherstellungsplans ist, verabschiedet werden können;

f) das Leitungsorgan genehmigt und überprüft regelmäßig die internen IKT-Revisionspläne des Finanzunternehmens, die IKT-Revision und die daran vorgenommenen wesentlichen Änderungen;

g) das Leitungsorgan weist angemessene Budgetmittel zu und überprüft diese regelmäßig, um den Anforderungen des Finanzunternehmens an die digitale operationale Resilienz in Bezug auf alle Arten von Ressourcen gerecht zu werden, einschließlich einschlägiger Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz nach Artikel 13 Absatz 6 sowie IKT-Kompetenzen für alle Mitarbeiter;

h) das Leitungsorgan genehmigt und überprüft regelmäßig die Leitlinie des Finanzunternehmens in Bezug auf Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die von IKT-Drittdienstleistern bereitgestellt werden;

i) das Leitungsorgan richtet auf Unternehmensebene Meldekanäle ein, die es ihm ermöglichen, ordnungsgemäß über Folgendes informiert zu werden:

   i) mit IKT-Drittdienstleistern geschlossene Vereinbarungen über die Nutzung von IKT-Dienstleistungen,

   ii) alle relevanten geplanten wesentlichen Änderungen in Bezug auf die IKT-Drittdienstleister,

   iii) die potenziellen Auswirkungen derartiger Änderungen auf die kritischen oder wichtigen Funktionen, die Gegenstand dieser Vereinbarungen sind, einschließlich einer Zusammenfassung der Risikoanalyse, um die Auswirkungen dieser Änderungen zu bewerten, und zumindest über schwerwiegende IKT-bezogene Vorfälle und deren Auswirkungen sowie über Gegen-, Wiederherstellungs- und Korrekturmaßnahmen.

(3) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, richten eine Funktion ein, um die mit IKT-Drittdienstleistern über die Nutzung von IKT-Dienstleistungen geschlossenen Vereinbarungen zu überwachen, oder benennen ein Mitglied der Geschäftsleitung, das für die Überwachung der damit verbundenen Risikoexposition und die einschlägige Dokumentation verantwortlich ist.

(4) Die Mitglieder des Leitungsorgans des Finanzunternehmens halten ausreichende Kenntnisse und Fähigkeiten aktiv auf dem neuesten Stand — unter anderem indem sie regelmäßig spezielle Schulungen absolvieren — entsprechend den zu managenden IKT-Risiken, um die IKT-Risiken und deren Auswirkungen auf die Geschäftstätigkeit des Finanzunternehmens verstehen und bewerten können.

Abschnitt II

Artikel 6

IKT-Risikomanagementrahmen

(1) Finanzunternehmen verfügen über einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen, der Teil ihres Gesamtrisikomanagementsystems ist und es ihnen ermöglicht, IKT-Risiken schnell, effizient und umfassend anzugehen und ein hohes Niveau an digitaler operationaler Resilienz zu gewährleisten.

(2) Der IKT-Risikomanagementrahmen umfasst mindestens Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle und -Tools, die erforderlich sind, um alle Informations- und IKT-Assets, einschließlich Computer-Software, Hardware und Server, ordnungsgemäß und angemessen zu schützen sowie um alle relevanten physischen Komponenten und Infrastrukturen, wie etwa Räumlichkeiten, Rechenzentren und ausgewiesene sensible Bereiche zu schützen, damit der angemessene Schutz aller Informations- und IKT-Assets vor Risiken, einschließlich der Beschädigung und des unbefugten Zugriffs oder der unbefugten Nutzung, gewährleistet ist.

(3) Im Einklang mit ihrem IKT-Risikomanagementrahmen minimieren Finanzunternehmen die Auswirkungen von IKT-Risiken, indem sie geeignete Strategien, Leit- und Richtlinien, Verfahren, IKT-Protokolle und Tools einsetzen. Sie legen den zuständigen Behörden auf Anfrage vollständige und aktuelle Informationen über IKT-Risiken und ihren IKT-Risikomanagementrahmen vor.

(4) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, übertragen die Zuständigkeit für das Management und die Überwachung des IKT-Risikos an eine Kontrollfunktion und stellen ein angemessenes Maß an Unabhängigkeit dieser Kontrollfunktion sicher, um Interessenkonflikte zu vermeiden. Die Finanzunternehmen sorgen für eine angemessene Trennung und Unabhängigkeit von IKT-Risikomanagementfunktionen, Kontrollfunktionen und internen Revisionsfunktionen gemäß dem Modell der drei Verteidigungslinien oder einem internen Modell für Risikomanagement und Kontrolle.

(5) Der IKT-Risikomanagementrahmen wird mindestens einmal jährlich — bzw. im Falle von Kleinstunternehmen regelmäßig — sowie bei Auftreten schwerwiegender IKT-bezogener Vorfälle und nach aufsichtsrechtlichen Anweisungen oder Feststellungen, die sich aus einschlägigen Tests der digitalen operationalen Resilienz oder Auditverfahren ergeben, dokumentiert und überprüft. Der Rahmen wird auf Grundlage der bei Umsetzung und Überwachung gewonnenen Erkenntnisse kontinuierlich verbessert. Der zuständigen Behörde wird auf deren Anfrage ein Bericht über die Überprüfung des IKT-Risikomanagementrahmens vorgelegt.

(6) Im Einklang mit dem Revisionsplan des betreffenden Finanzunternehmens ist der IKT-Risikomanagementrahmen von Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, regelmäßig einer internen Revision durch Revisoren zu unterziehen. Diese Revisoren verfügen über ausreichendes Wissen und ausreichende Fähigkeiten und Fachkenntnisse im Bereich IKT-Risiken sowie über eine angemessene Unabhängigkeit. Häufigkeit und Schwerpunkt von IKT-Revisionen sind den IKT-Risiken des Finanzunternehmens entsprechend angemessen.

(7) Auf der Grundlage der Feststellungen aus der Überprüfung der internen Revision legen Finanzunternehmen ein förmliches Follow-up-Verfahren einschließlich Regeln für die rechtzeitige Überprüfung und Auswertung kritischer Erkenntnisse der IKT-Revision fest.

(8) Der IKT-Risikomanagementrahmen umfasst eine Strategie für die digitale operationale Resilienz, in der dargelegt wird, wie der Rahmen umgesetzt wird. Zu diesem Zweck schließt die Strategie für die digitale operationale Resilienz Methoden, um IKT-Risiken anzugehen und spezifische IKT-Ziele zu erreichen, ein, indem

a) erläutert wird, wie der IKT-Risikomanagementrahmen die Geschäftsstrategie und die Ziele des Finanzunternehmens unterstützt;

b) die Risikotoleranzschwelle für IKT-Risiken im Einklang mit der Risikobereitschaft des Finanzunternehmens festgelegt und die Auswirkungsstoleranz mit Blick auf IKT-Störungen untersucht wird;

c) klare Ziele für die Informationssicherheit festgelegt werden, einschließlich der wesentlichen Leistungsindikatoren und der wesentlichen Risikokennzahlen;

d) die IKT-Referenzarchitektur und etwaige Änderungen erläutert werden, die für die Erreichung spezifischer Geschäftsziele erforderlich sind;

e) die verschiedenen Mechanismen dargelegt werden, die eingesetzt wurden, um IKT-bezogene Vorfälle zu erkennen, sich davor zu schützen und daraus entstehende Folgen zu verhindern;

f) der aktuelle Stand bezüglich der digitalen operationalen Resilienz anhand der Anzahl gemeldeter schwerwiegender IKT-Vorfälle und bezüglich der Wirksamkeit von Präventivmaßnahmen dargelegt wird;

g) Tests der digitalen operationalen Resilienz gemäß Kapitel IV dieser Verordnung durchgeführt werden;

h) für IKT-bezogene Vorfälle eine Kommunikationsstrategie dargelegt wird, die gemäß Artikel 14 offengelegt werden muss.

(9) Finanzunternehmen können im Zusammenhang mit der Strategie für die digitale operationale Resilienz nach Absatz 8 eine ganzheitliche Strategie zur Nutzung mehrerer IKT-Anbieter auf Gruppen- oder Unternehmensebene festlegen, in der wesentliche Abhängigkeiten von IKT-Drittdienstleistern aufgezeigt und die Gründe für die Nutzung verschiedener IKT-Drittdienstleister erläutert werden.

(10) 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 oder externe Unternehmen auslagern. Im Falle einer solchen Auslagerung bleibt das Finanzunternehmen weiterhin uneingeschränkt für die Überprüfung der Einhaltung der IKT-Risikomanagementanforderungen verantwortlich.

Artikel 7

IKT-Systeme, -Protokolle und -Tools

Um IKT-Risiken zu bewältigen und zu managen, verwenden und unterhalten Finanzunternehmen stets auf dem neuesten Stand zu haltende IKT-Systeme, -Protokolle und -Tools, die

a) dem Umfang von Vorgängen, die die Ausübung ihrer Geschäftstätigkeiten unterstützen, im Einklang mit dem Grundsatz der Verhältnismäßigkeit nach Artikel 4 angemessen sind;

b) zuverlässig sind;

c) mit ausreichenden Kapazitäten ausgestattet sind, um die Daten, die für die Ausführung von Tätigkeiten und die rechtzeitige Erbringung von Dienstleistungen erforderlich sind, genau zu verarbeiten und Auftragsspitzen, Mitteilungen oder Transaktionen auch bei Einführung neuer Technologien bewältigen zu können;

d) technologisch resilient sind, um dem unter angespannten Marktbedingungen oder anderen widrigen Umständen erforderlichen zusätzlichen Bedarf an Informationsverarbeitung angemessen zu begegnen.

Artikel 8

Identifizierung

(1) Als Teil des IKT-Risikomanagementrahmens gemäß Artikel 6 Absatz 1 ermitteln und klassifizieren Finanzunternehmen alle IKT-gestützten Unternehmensfunktionen, Rollen und Verantwortlichkeiten, die Informations- und IKT-Assets, die diese Funktionen unterstützen, sowie deren Rollen und Abhängigkeiten hinsichtlich der IKT-Risiken und dokumentieren sie angemessen. Finanzunternehmen überprüfen erforderlichenfalls, mindestens jedoch einmal jährlich, ob diese Klassifizierung und jegliche einschlägige Dokumentation angemessen sind.

(2) Finanzunternehmen ermitteln kontinuierlich alle Quellen für IKT-Risiken, insbesondere das Risiko gegenüber und von anderen Finanzunternehmen, und bewerten Cyberbedrohungen und IKT-Schwachstellen, die für ihre IKT-gestützten Geschäftsfunktionen, Informations- und IKT-Assets relevant sind. Finanzunternehmen überprüfen regelmäßig, mindestens jedoch einmal jährlich die sie betreffenden Risikoszenarien.

(3) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, führen bei jeder wesentlichen Änderung der Netzwerk- und Informationssysteminfrastruktur, der Prozesse oder Verfahren, die sich auf ihre IKT-gestützten Unternehmensfunktionen, Informations- oder IKT-Assets auswirken, eine Risikobewertung durch.

(4) Finanzunternehmen ermitteln alle Informations- und IKT-Assets, einschließlich derer an externen Standorten, Netzwerkressourcen und Hardware, und erfassen diejenigen, die als kritisch gelten. Sie erfassen die Konfiguration von Informations- und IKT-Assets sowie die Verbindungen und Interdependenzen zwischen den verschiedenen Informations- und IKT-Assets.

(5) Finanzunternehmen ermitteln und dokumentieren alle Prozesse, die von IKT-Drittdienstleistern abhängen, und ermitteln Vernetzungen mit IKT-Drittdienstleistern, die Dienste zur Unterstützung kritischer oder wichtiger Funktionen bereitstellen.

(6) Für die Zwecke der Absätze 1, 4 und 5 führen Finanzunternehmen entsprechende Inventare, die sie regelmäßig sowie bei jeder wesentlichen Änderung im Sinne von Absatz 3 aktualisieren.

(7) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, führen für alle IKT-Altsysteme regelmäßig, mindestens jedoch einmal jährlich und in jedem Fall vor und nach Anschluss von Technologien, Anwendungen oder Systemen eine spezifische Bewertung des IKT-Risikos durch.

Artikel 9

Schutz und Prävention

(1) Um einen angemessenen Schutz von IKT-Systemen zu gewährleisten und Gegenmaßnahmen zu organisieren, überwachen und kontrollieren Finanzunternehmen kontinuierlich die Sicherheit und das Funktionieren der IKT-Systeme und -Tools und minimieren durch den Einsatz angemessener IKT-Sicherheitstools, -Richtlinien und -Verfahren die Auswirkungen von IKT-Risiken auf IKT-Systeme.

(2) Finanzunternehmen konzipieren, beschaffen und implementieren IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools, die darauf abzielen, die Resilienz, Kontinuität und Verfügbarkeit von IKT-Systemen, insbesondere jener zur Unterstützung kritischer oder wichtiger Funktionen, zu gewährleisten und hohe Standards in Bezug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit, von Daten aufrechtzuerhalten, unabhängig davon, ob diese Daten gespeichert sind oder gerade verwendet oder übermittelt werden.

(3) Um die in Absatz 2 genannten Ziele zu erreichen, greifen Finanzunternehmen auf IKT-Lösungen und -Prozesse zurück, die gemäß Artikel 4 angemessen sind. Diese IKT-Lösungen und -Prozesse müssen

a) die Sicherheit der Datenübermittlungsmittel gewährleisten;

b) das Risiko von Datenkorruption oder -verlust, unbefugtem Zugriff und technischen Mängeln, die die Geschäftstätigkeit beeinträchtigen können, minimieren;

c) dem Mangel an Verfügbarkeit, der Beeinträchtigung der Authentizität und Integrität, den Verletzungen der Vertraulichkeit und dem Verlust von Daten vorbeugen;

d) gewährleisten, dass Daten vor Risiken, die beim Datenmanagement entstehen, einschließlich schlechter Verwaltung, verarbeitungsbedingter Risiken und menschlichem Versagen, geschützt werden.

(4) Als Teil des IKT-Risikomanagementrahmens nach Artikel 6 Absatz 1 gilt für Finanzunternehmen Folgendes:

a) Sie erarbeiten und dokumentieren eine Informationssicherheitsleitlinie, in der Regeln zum Schutz der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten und der Informations- und IKT-Assets, gegebenenfalls einschließlich derjenigen ihrer Kunden, festgelegt sind;

b) sie richten entsprechend einem risikobasierten Ansatz eine solide Struktur für Netzwerk- und Infrastrukturmanagement unter Verwendung angemessener Techniken, Methoden und Protokolle ein, wozu auch die Umsetzung automatisierter Mechanismen zur Isolierung betroffener Informationsassets im Falle von Cyberangriffen gehören kann;

c) sie implementieren Richtlinien, die den physischen oder logischen Zugang zu Informations- und IKT-Assets ausschließlich auf den Umfang beschränken, der für rechtmäßige und zulässige Funktionen und Tätigkeiten erforderlich ist, und legen zu diesem Zweck eine Reihe von Konzepten, Verfahren und Kontrollen fest, die auf Zugangs- und Zugriffsrechte gerichtet sind, und gewährleisten deren gründliche Verwaltung;

d) sie implementieren Konzepte und Protokolle für starke Authentifizierungsmechanismen, die auf einschlägigen Normen und speziellen Kontrollsystemen basieren, sowie Schutzmaßnahmen für kryptografische Schlüssel, wobei Daten auf der Grundlage der Ergebnisse aus genehmigten Datenklassifizierungs- und IKT-Risikobewertungsprozessen verschlüsselt werden;

e) sie implementieren und dokumentieren Richtlinien, Verfahren und Kontrollen für das IKT-Änderungsmanagement, einschließlich Änderungen an Software, Hardware, Firmware-Komponenten, den Systemen oder von Sicherheitsparametern, die auf einem Risikobewertungsansatz basieren und fester Bestandteil des gesamten Änderungsmanagementprozesses des Finanzunternehmens sind, um sicherzustellen, dass alle Änderungen an IKT-Systemen auf kontrollierte Weise erfasst, getestet, bewertet, genehmigt, implementiert und überprüft werden;

f) sie besitzen angemessene und umfassende dokumentierte Richtlinien für Patches und Updates.

Für die Zwecke von Unterabsatz 1 Buchstabe b konzipieren Finanzunternehmen die Infrastruktur für die Netzanbindung und Netzwerkverbindung so, dass sie sofort getrennt oder segmentiert werden kann, damit eine Ansteckung, insbesondere bei miteinander verbundenen Finanzprozessen, minimiert und verhindert wird.

Für die Zwecke von Unterabsatz 1 Buchstabe e wird das Verfahren für das IKT-Änderungsmanagement von zuständigen Leitungsebenen genehmigt und hat spezifische Protokolle.

Artikel 10

Erkennung

(1) Finanzunternehmen verfügen über Mechanismen, um anomale Aktivitäten im Einklang mit Artikel 17, darunter auch Probleme bei der Leistung von IKT-Netzwerken und IKT-bezogene Vorfälle, umgehend zu erkennen und potenzielle einzelne wesentliche Schwachstellen zu ermitteln.

Alle in Unterabsatz 1 aufgeführten Erkennungsmechanismen werden gemäß Artikel 25 regelmäßig getestet.

(2) Die in Absatz 1 genannten Erkennungsmechanismen ermöglichen mehrere Kontrollebenen und legen Alarmschwellen und -kriterien fest, um Reaktionsprozesse bei IKT-bezogenen Vorfällen auszulösen und einzuleiten, einschließlich automatischer Warnmechanismen für Mitarbeiter, die für Reaktionsmaßnahmen bei IKT-bezogenen Vorfällen zuständig sind.

(3) Finanzunternehmen stellen ausreichende Ressourcen und Kapazitäten bereit, um Nutzeraktivitäten, das Auftreten von IKT-Anomalien und IKT-bezogenen Vorfällen, darunter insbesondere Cyberangriffe, zu überwachen.

(4) Datenbereitstellungsdienste verfügen darüber hinaus über Systeme, mit denen wirksam Handelsauskünfte auf Vollständigkeit geprüft, Lücken und offensichtliche Fehler erkannt und eine Neuübermittlung angefordert werden können.

Artikel 11

Reaktion und Wiederherstellung

(1) Als Teil des in Artikel 6 Absatz 1 genannten IKT-Risikomanagementrahmens und auf der Grundlage der Identifizierungsanforderungen nach Artikel 8 legen Finanzunternehmen eine umfassende IKT-Geschäftsfortführungsleitlinie fest, die als eigenständige spezielle Leitlinie, die fester Bestandteil der allgemeinen Geschäftsfortführungsleitlinie des Finanzunternehmens ist, verabschiedet werden kann.

(2) Finanzunternehmen implementieren die IKT-Geschäftsfortführungsleitlinie mittels spezieller, angemessener und dokumentierter Regelungen, Pläne, Verfahren und Mechanismen, die darauf abzielen,

a) die Fortführung der kritischen oder wichtigen Funktionen des Finanzunternehmens sicherzustellen;

b) auf alle IKT-bezogenen Vorfälle rasch, angemessen und wirksam zu reagieren und diesen so entgegenzuwirken, dass Schäden begrenzt werden und die Wiederaufnahme von Tätigkeiten und Wiederherstellungsmaßnahmen Vorrang erhalten;

c) unverzüglich spezielle Pläne zu aktivieren, die Eindämmungsmaßnahmen, Prozesse und Technologien für alle Arten IKT-bezogener Vorfälle ermöglichen und weitere Schäden vermeiden, sowie maßgeschneiderte Verfahren zur Reaktion und Wiederherstellung gemäß Artikel 12 zu aktivieren;

d) vorläufige Auswirkungen, Schäden und Verluste einzuschätzen;

e) Kommunikations- und Krisenmanagementmaßnahmen festzulegen, die gewährleisten, dass allen relevanten internen Mitarbeitern und externen Interessenträgern im Sinne von Artikel 14 aktualisierte Informationen übermittelt werden, und die Meldung an die zuständigen Behörden gemäß Artikel 19 sicherstellen.

(3) Finanzunternehmen implementieren als Teil des in Artikel 6 Absatz 1 genannten IKT-Risikomanagementrahmens damit verbundene IKT-Reaktions- und Wiederherstellungspläne, die einer unabhängigen internen Revision zu unterziehen sind, sofern es sich bei dem Finanzunternehmen nicht um ein Kleinstunternehmen handelt.

(4) Finanzunternehmen erstellen, pflegen und testen regelmäßig angemessene IKT-Geschäftsfortführungspläne, insbesondere in Bezug auf kritische oder wichtige Funktionen, die ausgelagert oder durch vertragliche Vereinbarungen an IKT-Drittdienstleister vergeben werden.

(5) Als Teil der allgemeinen Geschäftsfortführungsleitlinie führen Finanzunternehmen eine Business-Impact-Analyse (BIA) der bestehenden Risiken für schwerwiegende Betriebsstörungen durch. Im Rahmen der BIA bewerten Finanzunternehmen die potenziellen Auswirkungen schwerwiegender Betriebsstörungen anhand quantitativer und qualitativer Kriterien, wobei sie gegebenenfalls interne und externe Daten und Szenarioanalysen heranziehen. Dabei werden die Kritikalität der identifizierten und erfassten Unternehmensfunktionen, Unterstützungsprozesse, Abhängigkeiten von Dritten und Informationsassets sowie deren Interdependenzen berücksichtigt. Die Finanzunternehmen stellen sicher, dass IKT-Assets und -Dienste in voller Übereinstimmung mit der BIA konzipiert und genutzt werden, insbesondere wenn es darum geht, die Redundanz aller kritischen Komponenten in angemessener Weise zu gewährleisten.

(6) Im Rahmen ihres umfassenden IKT-Risikomanagements gilt für Finanzunternehmen Folgendes:

a) sie testen bei IKT-Systemen, die alle Funktionen unterstützen, mindestens jährlich sowie im Falle jeglicher wesentlicher Änderungen an IKT-Systemen, die kritische oder wichtige Funktionen unterstützen, die IKT-Geschäftsfortführungspläne sowie die IKT-Reaktions- und Wiederherstellungspläne;

b) sie testen die gemäß Artikel 14 erstellten Krisenkommunikationspläne.

Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, nehmen für die Zwecke von Unterabsatz 1 Buchstabe a Szenarien für Cyberangriffe und Umstellungen von der primären IKT-Infrastruktur auf die redundanten Kapazitäten, Backups und Systeme, die für die Erfüllung der Verpflichtungen nach Artikel 12 erforderlich sind, in ihre Testpläne auf.

Finanzunternehmen überprüfen ihre IKT-Geschäftsfortführungsleitlinie und ihre IKT-Reaktions- und Wiederherstellungspläne regelmäßig und berücksichtigen dabei die Ergebnisse von Tests, die gemäß Unterabsatz 1 durchgeführt wurden, sowie die Empfehlungen, die sich aus Audits oder aufsichtlichen Überprüfungen ergeben.

(7) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, verfügen über eine Krisenmanagementfunktion, die bei Aktivierung ihrer IKT- Geschäftsfortführungspläne oder ihrer IKT-Reaktions- und Wiederherstellungspläne unter anderem klare Verfahren für die Abwicklung interner und externer Krisenkommunikation gemäß Artikel 14 festlegt.

(8) Finanzunternehmen sorgen dafür, dass Aufzeichnungen über die Tätigkeiten vor und während Störungen, wenn ihre IKT-Geschäftsfortführungspläne oder ihre IKT-Reaktions- und Wiederherstellungspläne aktiviert werden, jederzeit eingesehen werden können.

(9) Zentralverwahrer übermitteln den zuständigen Behörden Kopien der Ergebnisse der Tests der IKT-Geschäftsfortführung oder ähnlicher Vorgänge.

(10) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, melden den zuständigen Behörden auf Anfrage die geschätzten aggregierten jährlichen Kosten und Verluste, die durch schwerwiegende IKT-bezogene Vorfälle verursacht wurden.

(11) Gemäß jeweils Artikel 16 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 arbeiten die Europäischen Aufsichtsbehörden (im Folgenden „ESA“) über den Gemeinsamen Ausschuss bis zum 17. Juli 2024 gemeinsame Leitlinien für die Schätzung der aggregierten jährlichen Kosten und Verluste nach Absatz 10 aus.

Artikel 12

Richtlinie und Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung

(1) Um die Wiederherstellung von IKT-Systemen und Daten mit minimaler Ausfallzeit sowie begrenzten Störungen und Verlusten als Teil ihres IKT-Risikomanagementrahmens sicherzustellen, entwickeln und dokumentieren Finanzunternehmen:

a) Richtlinien und Verfahren für die Datensicherung, in denen der Umfang der Daten, die der Sicherung unterliegen, und die Mindesthäufigkeit der Sicherung auf der Grundlage der Kritikalität der Informationen oder des Vertraulichkeitsgrads der Daten festgelegt werden;

b) Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden.

(2) Finanzunternehmen richten Datensicherungssysteme ein, die in Übereinstimmung mit den Richtlinien und Verfahren zur Datensicherung sowie den Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung aktiviert werden können. Die Aktivierung von Datensicherungssystemen darf die Sicherheit der Netzwerk- und Informationssysteme oder die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten nicht gefährden. Die Datensicherungsverfahren sowie die Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden sind regelmäßig zu testen.

(3) Bei der Wiedergewinnung gesicherter Daten mithilfe eigener Systeme verwenden Finanzunternehmen IKT-Systeme, die von ihrem Quellsystem physisch und logisch getrennt sind. Die IKT-Systeme müssen sicher vor unbefugtem Zugriff oder IKT-Manipulationen geschützt sein und die rechtzeitige Wiederherstellung von Diensten ermöglichen, wobei erforderlichenfalls Daten- und Systemsicherungen (Backups) zu nutzen sind.

Bei zentralen Gegenparteien ermöglichen die Wiederherstellungspläne die Wiederherstellung aller zum Zeitpunkt der Störung laufenden Transaktionen, damit die zentrale Gegenpartei weiterhin sicher arbeiten und die Abwicklung zum vorgesehenen Zeitpunkt abschließen kann.

Datenbereitstellungsdienste unterhalten zusätzlich angemessene Ressourcen und verfügen über die entsprechenden Sicherungs- und Wiedergewinnungseinrichtungen, damit ihre Dienste jederzeit angeboten und aufrechterhalten werden können.

(4) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, unterhalten redundante IKT-Kapazitäten mit Ressourcen, Fähigkeiten und Funktionen, die für die Deckung des Geschäftsbedarfs ausreichen und angemessen sind. Kleinstunternehmen bewerten auf der Grundlage ihres Risikoprofils, ob diese redundanten IKT-Kapazitäten unterhalten werden müssen.

(5) Zentralverwahrer unterhalten mindestens einen sekundären Verarbeitungsstandort, dessen Ressourcen, Kapazitäten, Funktionen und Personalressourcen angemessen sind, um den Geschäftsbedarf zu decken.

Der sekundäre Verarbeitungsstandort

a) befindet sich in geografischer Entfernung vom primären Verarbeitungsstandort, damit er ein eigenes Risikoprofil aufweist und nicht von dem Ereignis, das sich am primären Standort ereignet hat, betroffen ist;

b) kann die Kontinuität kritischer oder wichtiger, mit dem primären Standort identischer Funktionen gewährleisten oder ein Leistungsniveau bereitstellen, mit dem sichergestellt wird, dass das Finanzunternehmen seine kritischen Vorgänge im Rahmen der Wiederherstellungsziele durchführt;

c) ist für das Personal des Finanzunternehmens unmittelbar zugänglich, damit die Kontinuität kritischer oder wichtiger Funktionen gewährleistet werden kann, falls der primäre Verarbeitungsstandort nicht mehr zur Verfügung steht.

(6) Bei der Festlegung der Vorgaben für die Wiederherstellungszeit und die Wiederherstellungspunkte jeder Funktion berücksichtigen die Finanzunternehmen, ob es sich um eine kritische oder wichtige Funktion handelt, sowie die potenziellen Gesamtauswirkungen auf die Markteffizienz. Mit diesen Zeitvorgaben ist sichergestellt, dass die vereinbarte Dienstleistungsgüte in Extremszenarien erreicht werden.

(7) Bei der Wiederherstellung nach IKT-bezogenen Vorfällen führen Finanzunternehmen die erforderlichen Prüfungen durch, einschließlich jeglicher Mehrfachprüfungen und Abgleiche, um die größtmögliche Datenintegrität sicherzustellen. Diese Prüfungen werden auch bei der Rekonstruktion von Daten externer Interessenträger durchgeführt, um sicherzustellen, dass alle Daten systemübergreifend einheitlich sind.

Artikel 13

Lernprozesse und Weiterentwicklung

(1) Finanzunternehmen verfügen über Kapazitäten und Personal, um Informationen über Schwachstellen und Cyberbedrohungen, IKT-bezogene Vorfälle, insbesondere Cyberangriffe, zu sammeln und ihre wahrscheinlichen Auswirkungen auf ihre digitale operationale Resilienz zu untersuchen.

(2) Nach Störungen ihrer Haupttätigkeiten infolge schwerwiegender IKT-bezogener Vorfälle sehen Finanzunternehmen nachträgliche Prüfungen IKT-bezogener Vorfälle vor, die die Ursachen für Störungen untersuchen und die erforderlichen Verbesserungen an IKT-Vorgängen oder im Rahmen der in Artikel 11 genannten IKT-Geschäftsfortführungsleitlinie identifizieren.

Finanzunternehmen, die keine Kleinstunternehmen sind, teilen den zuständigen Behörden auf Verlangen die Änderungen mit, die nach der Prüfung IKT-bezogener Vorfälle gemäß Unterabsatz 1 vorgenommen wurden.

Bei den in Unterabsatz 1 genannten nachträglichen Prüfungen IKT-bezogener Vorfälle wird ermittelt, ob die festgelegten Verfahren befolgt und die ergriffenen Maßnahmen wirksam waren, unter anderem in Bezug auf:

a) die Schnelligkeit bei der Reaktion auf Sicherheitswarnungen und bei der Bestimmung der Auswirkungen von IKT-bezogenen Vorfällen und ihrer Schwere;

b) die Qualität und Schnelligkeit bei der Durchführung forensischer Analysen, sofern dies als zweckmäßig erachtet wird;

c) die Wirksamkeit der Eskalation von Vorfällen innerhalb des Finanzunternehmens;

d) die Wirksamkeit interner und externer Kommunikation.

(3) Erkenntnisse aus gemäß den Artikeln 26 und 27 durchgeführten Tests der digitalen operationalen Resilienz und aus realen IKT-bezogenen Vorfällen, insbesondere Cyberangriffen, werden neben Herausforderungen, die sich bei der Aktivierung von IKT- Geschäftsfortführungsplänen und IKT-Reaktions- und Wiederherstellungsplänen ergeben, zusammen mit einschlägigen Informationen, die mit Gegenparteien ausgetauscht und im Rahmen aufsichtlicher Überprüfungen bewertet werden, kontinuierlich ordnungsgemäß in den IKT-Risikobewertungsprozess einbezogen. Diese Erkenntnisse bilden die Grundlage für angemessene Überprüfungen relevanter Komponenten des IKT-Risikomanagementrahmens gemäß Artikel 6 Absatz 1.

(4) Finanzunternehmen überwachen die Wirksamkeit der Umsetzung ihrer Strategie für die digitale operationale Resilienz gemäß Artikel 6 Absatz 8. Dabei erfassen sie die Entwicklung der IKT-Risiken im Zeitverlauf, untersuchen Häufigkeit, Art, Ausmaß und Entwicklung IKT-bezogener Vorfälle, insbesondere Cyberangriffe und deren Muster, um das Ausmaß der IKT-Risiken — insbesondere in Bezug auf kritische oder wichtige Funktionen — zu verstehen und die Cyberreife und die Abwehrbereitschaft des Finanzunternehmens zu verbessern.

(5) Leitende IKT-Mitarbeiter erstatten dem Leitungsorgan mindestens einmal jährlich über die in Absatz 3 genannten Feststellungen Bericht und geben Empfehlungen ab.

(6) Finanzunternehmen entwickeln Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz, die im Rahmen ihrer Programme für die Mitarbeiterschulung obligatorisch sind. Diese Programme und Schulungen gelten für alle Beschäftigten und die Geschäftsleitung und sind so komplex, dass sie deren jeweiligem Aufgabenbereich angemessen sind. Gegebenenfalls nehmen die Finanzunternehmen entsprechend Artikel 30 Absatz 2 Buchstabe i auch IKT-Drittdienstleister in ihre einschlägigen Schulungsprogramme auf.

(7) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, überwachen einschlägige technologische Entwicklungen fortlaufend — auch um die möglichen Auswirkungen des Einsatzes solcher neuen Technologien auf die Anforderungen an die IKT-Sicherheit und die digitale operationale Resilienz zu verstehen. Sie halten sich über die neuesten Prozesse für das IKT-Risikomanagement auf dem Laufenden, um gegenwärtige oder neue Formen von Cyberangriffen wirksam abzuwehren.

Artikel 14

Kommunikation

(1) Als Teil des IKT-Risikomanagementrahmens gemäß Artikel 6 Absatz 1 verfügen Finanzunternehmen über Kommunikationspläne, die je nach Sachlage eine verantwortungsbewusste Offenlegung zumindest von schwerwiegenden IKT-bezogenen Vorfällen oder Schwachstellen gegenüber Kunden und anderen Finanzunternehmen sowie der Öffentlichkeit ermöglichen.

(2) Als Teil des IKT-Risikomanagementrahmens setzen Finanzunternehmen Kommunikationsstrategien für interne Mitarbeiter und externe Interessenträger um. Bei Kommunikationsleitlinien für Mitarbeiter wird berücksichtigt, dass zwischen dem Personal, das am IKT-Risikomanagement, insbesondere im Bereich Reaktion und Wiederherstellung, beteiligt ist, und dem zu informierendem Personal unterschieden werden muss.

(3) Mindestens eine Person im Finanzunternehmen ist mit der Umsetzung der Kommunikationsstrategie für IKT-bezogene Vorfälle beauftragt und nimmt zu diesem Zweck die entsprechende Aufgabe gegenüber der Öffentlichkeit und den Medien wahr.

Artikel 15

Weitere Harmonisierung von Tools, Methoden, Prozessen und Richtlinien für IKT-Risikomanagement

Die ESA entwickeln über den Gemeinsamen Ausschuss in Abstimmung mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) gemeinsame Entwürfe technischer Regulierungsstandards für folgende Zwecke:

a) die Festlegung weiterer Elemente, die in die in Artikel 9 Absatz 2 genannten Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit aufzunehmen sind, um die Sicherheit von Netzwerken zu gewährleisten, angemessene Schutzvorrichtungen gegen Eindringen und Missbrauch von Daten zu ermöglichen, die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten, einschließlich kryptografischer Techniken, zu wahren und eine präzise und rasche Datenübermittlung ohne wesentliche Störungen und unangemessene Verzögerungen zu gewährleisten;

b) die Entwicklung weiterer Komponenten der Kontrollen von Zugangs- und Zugriffsrechten gemäß Artikel 9 Absatz 4 Buchstabe c und der damit verbundenen Personalpolitik, mit denen Zugangsrechte, Verfahren für Erteilung und Widerruf von Rechten, die Überwachung anomalen Verhaltens in Bezug auf IKT-Risiken durch angemessene Indikatoren — auch für Netzwerknutzungsmuster, Zeiten, IT-Aktivität und unbekannte Geräte — spezifiziert werden;

c) die Weiterentwicklung der in Artikel 10 Absatz 1 genannten Mechanismen, die eine umgehende Erkennung anomaler Aktivitäten ermöglichen, sowie der in Artikel 10 Absatz 2 genannten Kriterien, die Verfahren für die Erkennung IKT-bezogener Vorfälle und die damit verbundenen Reaktionsprozesse auslösen;

d) die Spezifizierung der in Artikel 11 Absatz 1 genannten Komponenten der IKT-Geschäftsfortführungsleitlinie;

e) die Spezifizierung der Tests von IKT-Geschäftsfortführungsplänen gemäß Artikel 11 Absatz 6, damit bei diesen Tests Szenarien, in denen die Qualität der Bereitstellung einer kritischen oder wichtigen Funktion auf ein inakzeptables Niveau absinkt oder diese Funktion ganz ausfällt, und die potenziellen Auswirkungen der Insolvenz oder sonstiger Ausfälle einschlägiger IKT-Drittdienstleister sowie gegebenenfalls die etwaigen politischen Risiken in den Rechtsordnungen in den Ländern und Gebieten der jeweiligen Anbieter gebührend berücksichtigt werden;

f) die Spezifizierung der Komponenten der in Artikel 11 Absatz 3 genannten IKT-Reaktions- und Wiederherstellungspläne;

g) die Spezifizierung von Inhalt und Form des in Artikel 6 Absatz 5 genannten Berichts über die Überprüfung des IKT-Risikomanagementrahmens.

Bei der Entwicklung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte, wobei sie etwaigen Besonderheiten, die sich aus der unterschiedlichen Art der Tätigkeiten in verschiedenen Finanzdienstleistungssektoren ergeben, gebührend Rechnung tragen.

Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Absatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Artikel 16

Vereinfachter IKT-Risikomanagementrahmen

(1) Artikel 5 bis 15 gelten nicht für kleine und nicht verflochtene Wertpapierfirmen, entsprechend der Richtlinie (EU) 2015/2366 ausgenommene Zahlungsinstitute, entsprechend der Richtlinie 2013/36/EU ausgenommene Institute, für die die Mitgliedstaaten beschlossen haben, nicht von der in Artikel 2 Absatz 4 der vorliegenden Verordnung genannten Möglichkeit Gebrauch zu machen, nach der Richtlinie 2009/110/EG ausgenommene E-Geld-Institute und kleine Einrichtungen der betrieblichen Altersversorgung.

Unbeschadet des Unterabsatzes 1 müssen die in Unterabsatz 1 genannten Stellen

a) einen soliden und dokumentierten IKT-Risikomanagementrahmen errichten und aufrechterhalten, in dem die Mechanismen und Maßnahmen für ein rasches, effizientes und umfassendes Management des IKT-Risikos, einschließlich des Schutzes der einschlägigen physischen Komponenten und Infrastrukturen, detailliert sind;

b) die Sicherheit und das Funktionieren aller IKT-Systeme fortlaufend überwachen;

c) die Auswirkungen von IKT-Risiken minimieren, indem solide, resiliente und aktualisierte IKT-Systeme, -Protokolle und -Tools, die zur Unterstützung der Durchführung ihrer Tätigkeiten und zur Bereitstellung von Diensten angemessen sind, verwendet werden, und in angemessener Weise die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten in den Netzwerk- und Informationssystemen schützen;

d) eine rasche Ermittlung und Aufdeckung der Ursachen von IKT-Risiken und -Anomalien in den Netzwerk- und Informationssystemen sowie eine rasche Handhabung von IKT-Vorfällen ermöglichen;

e) die wesentlichen Abhängigkeiten von IKT-Drittdienstleistern ermitteln;

f) die Kontinuität kritischer oder wichtiger Funktionen durch Geschäftsfortführungspläne sowie Gegen- und Wiederherstellungsmaßnahmen, die zumindest Sicherungs- und Wiedergewinnungsmaßnahmen umfassen, gewährleisten;

g) die unter Buchstabe f genannten Pläne und Maßnahmen sowie die Wirksamkeit der gemäß den Buchstaben a und c durchgeführten Kontrollen regelmäßig testen;

h) gegebenenfalls die relevanten operativen Schlussfolgerungen, die sich aus den Tests gemäß Buchstabe g und der Analyse nach einem Vorfall ergeben, in den IKT-Risikobewertungsprozess einbeziehen und entsprechend dem Bedarf und dem IKT-Risikoprofil Programme zur Sensibilisierung für IKT-Sicherheit sowie Schulungen zur digitalen operationalen Resilienz für Personal und Management entwickeln.

(2) Der in Absatz 1 Unterabsatz 2 Buchstabe a genannte IKT-Risikomanagementrahmen wird regelmäßig und bei Auftreten schwerwiegender IKT-bezogener Vorfälle entsprechend den aufsichtsrechtlichen Anweisungen dokumentiert und überprüft. Der Rahmen wird auf der Grundlage der bei Umsetzung und Überwachung gewonnenen Erkenntnisse kontinuierlich verbessert. Der zuständigen Behörde wird auf Anfrage ein Bericht über die Überprüfung des IKT-Risikomanagementrahmens vorgelegt.

(3) Die ESA entwickeln über den Gemeinsamen Ausschuss in Abstimmung mit der ENISA gemeinsame Entwürfe technischer Regulierungsstandards für die folgenden Zwecke:

a) Spezifizierung der Elemente, die in den in Absatz 1 Unterabsatz 1 Buchstabe a genannten IKT-Risikomanagementrahmen aufzunehmen sind;

b) Spezifizierung der Elemente in Bezug auf Systeme, Protokolle und Tools zur Minimierung der in Absatz 1 Unterabsatz 2 Buchstabe c genannten Auswirkungen von IKT-Risiken, um die Sicherheit der Netzwerke zu gewährleisten, angemessene Schutzvorkehrungen gegen Eindringen und Datenmissbrauch zu ermöglichen und die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten zu wahren;

c) Spezifizierung der Komponenten der in Absatz 1 Unterabsatz 2 Buchstabe f genannten IKT-Geschäftsfortführungspläne;

d) Spezifizierung der Vorschriften über die Tests der Geschäftsfortführungspläne und Gewährleistung der Wirksamkeit der Kontrollen gemäß Absatz 1 Unterabsatz 2 Buchstabe g und Gewährleistung, dass bei diesen Tests Szenarien, in denen die Qualität der Bereitstellung einer kritischen oder wichtigen Funktion auf ein inakzeptables Niveau absinkt oder diese Funktion ganz ausfällt, gebührend berücksichtigt werden;

e) nähere Spezifizierung von Inhalt und Form des in Absatz 2 genannten Berichts über die Überprüfung des IKT-Risikomanagementrahmens.

Bei der Entwicklung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte.

Die ESA übermitteln der Kommission die Entwürfe dieser technischen Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

KAPITEL III

Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle

Artikel 17

Prozess für die Behandlung IKT-bezogener Vorfälle

(1) Finanzunternehmen bestimmen einen Prozess für die Behandlung IKT-bezogener Vorfälle, richten diese ein und wenden sie an, um IKT-bezogene Vorfälle zu erkennen, zu behandeln und zu melden.

(2) Finanzunternehmen erfassen alle IKT-bezogenen Vorfälle und erheblichen Cyberbedrohungen. Finanzunternehmen richten angemessene Verfahren und Prozesse ein, um die kohärente und integrierte Überwachung, Handhabung und Weiterverfolgung IKT-bezogener Vorfälle zu gewährleisten, um sicherzustellen, dass Ursachen ermittelt, dokumentiert und angegangen werden, um das Auftreten solcher Vorfälle zu verhindern.

(3) Durch den in Absatz 1 genannten Prozess für die Behandlung IKT-bezogener Vorfälle

a) werden Frühwarnindikatoren eingesetzt;

b) werden Verfahren zur Ermittlung, Nachverfolgung, Protokollierung, Kategorisierung und Klassifizierung IKT-bezogener Vorfälle entsprechend ihrer Priorität und Schwere und entsprechend der Kritikalität der betroffenen Dienste entsprechend den in Artikel 18 Absatz 1 genannten Kriterien eingerichtet;

c) werden Funktionen und Zuständigkeiten zugewiesen, die bei verschiedenen Arten von IKT-bezogenen Vorfällen und -Szenarien aktiviert werden müssen;

d) werden gemäß Artikel 14 Pläne für die Kommunikation mit Personal, externen Interessenträgern und Medien sowie für die Benachrichtigung von Kunden, für interne Eskalationsverfahren, einschließlich IKT-bezogener Kundenbeschwerden, und für die Bereitstellung von Informationen an andere Finanzunternehmen, die als Gegenparteien fungieren, ausgearbeitet, je nach Sachlage;

e) wird sichergestellt, dass zumindest schwerwiegende IKT-bezogene Vorfälle der zuständigen höheren Führungsebene gemeldet werden und die Geschäftsleitung informiert wird, wobei die Auswirkungen und Gegenmaßnahmen und zusätzliche Kontrollen erläutert werden, die infolge dieser IKT-bezogenen Vorfälle einzurichten sind;

f) werden Verfahren für Reaktionsmaßnahmen bei IKT-bezogenen Vorfällen eingerichtet, um Auswirkungen zu mindern und sicherzustellen, dass die Dienste zeitnah verfügbar und sicher werden.

Artikel 18

Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen

(1) Finanzunternehmen klassifizieren IKT-bezogene Vorfälle und bestimmen deren Auswirkungen anhand folgender Kriterien:

a) Anzahl und/oder Relevanz der Kunden oder anderer Gegenparteien im Finanzbereich, die von dem IKT-bezogenen Vorfall betroffen sind, und gegebenenfalls des Werts oder der Anzahl der davon betroffenen Transaktionen und ob der IKT-bezogene Vorfall einen Reputationsschaden verursacht hat;

b) Dauer des IKT-bezogenen Vorfalls, einschließlich der Ausfallzeiten des Dienstes;

c) geografische Ausbreitung der von dem IKT-bezogenen Vorfall betroffenen Gebiete, insbesondere wenn mehr als zwei Mitgliedstaaten betroffen sind;

d) die mit dem IKT-bezogenen Vorfall verbundenen Verfügbarkeits-, Authentizitäts-, Integritäts- oder Vertraulichkeitsverluste von Daten;

e) Kritikalität der betroffenen Dienste, einschließlich der Transaktionen und Geschäfte des Finanzunternehmens;

f) wirtschaftliche Auswirkungen — insbesondere direkte und indirekte Kosten und Verluste — des IKT-bezogenen Vorfalls auf absoluter und relativer Basis.

(2) Finanzunternehmen stufen Cyberbedrohungen auf der Grundlage der Kritikalität der risikobehafteten Dienste, einschließlich der Transaktionen und Geschäfte des Finanzunternehmens, der Anzahl und/oder Relevanz der betroffenen Kunden oder Gegenparteien im Finanzbereich und der geografischen Ausbreitung der Risikogebiete als erheblich ein.

(3) Die ESA erarbeiten über den Gemeinsamen Ausschuss in Abstimmung mit der EZB und der ENISA gemeinsame Entwürfe technischer Regulierungsstandards, in denen Folgendes präzisiert wird:

a) die in Absatz 1 genannten Kriterien, einschließlich der Wesentlichkeitsschwellen für die Bestimmung schwerwiegender IKT-bezogener Vorfälle oder gegebenenfalls schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle, die der Meldepflicht nach Artikel 19 Absatz 1 unterliegen;

b) die Kriterien, die von den zuständigen Behörden anzuwenden sind, um die Relevanz schwerwiegender IKT-bezogener Vorfälle oder gegebenenfalls schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle für die jeweils zuständigen Behörden in anderen Mitgliedstaaten zu bewerten, sowie die Einzelheiten in den Meldungen über schwerwiegende IKT-bezogene Vorfälle oder gegebenenfalls schwerwiegende zahlungsbezogene Betriebs- oder Sicherheitsvorfälle, die anderen zuständigen Behörden gemäß Artikel 19 Absätze 6 und 7 übermittelt werden müssen;

c) die in Absatz 2 genannten Kriterien, einschließlich hoher Wesentlichkeitsschwellen für die Bestimmung erheblicher Cyberbedrohungen.

(4) Bei der Ausarbeitung der in Absatz 3 genannten gemeinsamen Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die in Artikel 4 Absatz 2 genannten Kriterien sowie von der ENISA entwickelte und veröffentlichte internationale Standards, Leitlinien und Spezifikationen, gegebenenfalls einschließlich Spezifikationen für andere Wirtschaftszweige. Für die Zwecke der Anwendung der in Artikel 4 Absatz 2 festgelegten Kriterien berücksichtigen die ESA gebührend, dass Kleinstunternehmen sowie kleine und mittlere Unternehmen ausreichende Ressourcen und Kapazitäten mobilisieren können müssen, um sicherzustellen, dass IKT-bezogene Vorfälle rasch bewältigt werden.

Die ESA übermitteln der Kommission diese allgemeinen Entwürfe technischer Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, diese Verordnung durch Annahme der in Absatz 3 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Artikel 19

Meldung schwerwiegender IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyberbedrohungen

(1) Finanzunternehmen melden der nach Artikel 46 jeweils zuständigen Behörde gemäß Absatz 4 schwerwiegende IKT-bezogene Vorfälle.

Unterliegt ein Finanzunternehmen der Aufsicht mehr als einer nach Artikel 46 zuständigen nationalen Behörde, so benennen die Mitgliedstaaten eine einzige zuständige Behörde als einschlägige zuständige Behörde, die für die Wahrnehmung der im vorliegenden Artikel aufgeführten Funktionen und Aufgaben verantwortlich ist.

Kreditinstitute, die gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 als bedeutend eingestuft wurden, melden schwerwiegende IKT-bezogene Vorfälle der gemäß Artikel 4 der Richtlinie 2013/36/EU benannten jeweils zuständigen nationalen Behörde, die diese Meldung unverzüglich an die EZB weiterleitet.

Für die Zwecke von Unterabsatz 1 erstellen Finanzunternehmen nach Erfassung und Analyse aller relevanten Informationen unter Verwendung der in Artikel 20 genannten Vorlage die Erstmeldung und die Meldungen nach Absatz 4 und übermitteln diese der zuständigen Behörde. Falls es aus technischen Gründen nicht möglich ist, die Erstmeldung unter Verwendung der Vorlage zu übermitteln, teilen die Finanzunternehmen dies der zuständigen Behörde auf anderem Wege mit.

Die Erstmeldung und die Meldungen nach Absatz 4 enthalten alle Informationen, die die zuständige Behörde benötigt, um die Signifikanz des schwerwiegenden IKT-bezogenen Vorfalls zu ermitteln und mögliche grenzüberschreitende Auswirkungen zu bewerten.

Unbeschadet der Meldung gemäß Unterabsatz 1 durch das Finanzunternehmen an die jeweils zuständige Behörde können die Mitgliedstaaten zusätzlich festlegen, dass einige oder alle Finanzunternehmen die Erstmeldung und jede Meldung nach Absatz 4 auch den gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden oder Computer-Notfallteams (computer security incident response teams — CSIRT) unter Verwendung der in Artikel 20 genannten Vorlage zur Verfügung stellen müssen.

(2) Finanzunternehmen können der jeweils zuständigen Behörde auf freiwilliger Basis erhebliche Cyberbedrohungen melden, wenn sie der Auffassung sind, dass die Bedrohung für das Finanzsystem, die Dienstnutzer oder die Kunden relevant ist. Die jeweils zuständige Behörde kann derartige Informationen anderen in Absatz 6 genannten einschlägigen Behörden zur Verfügung stellen.

Kreditinstitute, die gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 als bedeutend eingestuft wurden, können erhebliche Cyberbedrohungen auf freiwilliger Basis der gemäß Artikel 4 der Richtlinie 2013/36/EU benannten jeweils zuständigen nationalen Behörde melden, die diese Meldung unverzüglich an die EZB weiterleitet.

Die Mitgliedstaaten können festlegen, dass die Finanzunternehmen, die auf freiwilliger Basis eine Meldung gemäß Unterabsatz 1 vornehmen, diese Meldung auch an die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten CSIRT erstatten können.

(3) Wenn ein schwerwiegender IKT-bezogener Vorfall auftritt und Auswirkungen auf die finanziellen Interessen von Kunden hat, unterrichten die Finanzunternehmen, sobald sie hiervon Kenntnis erlangt haben, ihre Kunden unverzüglich über den schwerwiegenden IKT-bezogenen Vorfall und die Maßnahmen, die ergriffen wurden, um die nachteiligen Auswirkungen eines solchen Vorfalls zu mindern.

Im Falle einer erheblichen Cyberbedrohung unterrichten die Finanzunternehmen gegebenenfalls ihre potenziell betroffenen Kunden über angemessene Schutzmaßnahmen, die diese ergreifen könnten.

(4) Finanzunternehmen legen innerhalb der in Artikel 20 Absatz 1 Buchstabe a Ziffer ii festzulegenden Fristen der jeweils zuständigen Behörde Folgendes vor:

a) eine Erstmeldung;

b) nach der Erstmeldung gemäß Buchstabe a eine Zwischenmeldung, sobald sich der Status des ursprünglichen Vorfalls erheblich geändert hat oder sich die Handhabung des schwerwiegenden IKT-bezogenen Vorfalls auf der Grundlage neuer verfügbarer Informationen geändert hat, gegebenenfalls gefolgt von aktualisierten Meldungen, wann immer eine entsprechende Statusaktualisierung vorliegt, sowie auf ausdrücklichen Antrag der zuständigen Behörde;

c) eine Abschlussmeldung, wenn die Ursachenanalyse abgeschlossen ist — unabhängig davon, ob bereits Minderungsmaßnahmen getroffen wurden oder nicht — und sich die tatsächlichen Auswirkungen beziffern lassen und Schätzungen ersetzen.

(5) Finanzunternehmen dürfen im Einklang mit den sektorspezifischen Rechtsvorschriften der Union und der Mitgliedstaaten die Meldepflichten nach diesem Artikel an einen Drittdienstleister auslagern. Bei einer solchen Auslagerung bleibt das Finanzunternehmen in vollem Umfang für die Erfüllung der Anforderungen für die Meldung von Vorfällen verantwortlich.

(6) Nach Eingang der Erstmeldung und jeder Meldung nach Absatz 4 übermittelt die zuständige Behörde auf der Grundlage der je nach Sachlage bestehenden jeweiligen Zuständigkeiten zeitnah Einzelheiten zu dem schwerwiegenden IKT-bezogenen Vorfall an die folgenden Empfänger:

a) die EBA, die ESMA oder die EIOPA;

b) die EZB, sofern es sich um Finanzunternehmen im Sinne von Artikel 2 Absatz 1 Buchstaben a, b und d handelt;

c) die zuständigen Behörden, die zentrale Anlaufstelle oder die CSIRT, die jeweils gemäß der Richtlinie (EU) 2022/2555 benannt oder eingerichtet werden;

d) die in Artikel 3 der Richtlinie 2014/59/EU genannten Abwicklungsbehörden und den Einheitlichen Abwicklungsausschuss (Single Resolution Board — SRB) in Bezug auf die in Artikel 7 Absatz 2 der Verordnung (EU) Nr. 806/2014 des Europäischen Parlaments und des Rates ([37]) genannten Unternehmen sowie in Bezug auf die in Artikel 7 Absatz 4 Buchstabe b und Absatz 5 der Verordnung (EU) Nr. 806/2014 genannten Unternehmen und Gruppen, wenn diese Einzelheiten Vorfälle betreffen, die ein Risiko für die Sicherstellung kritischer Funktionen im Sinne von Artikel 2 Absatz 1 Nummer 35 der Richtlinie 2014/59/EU darstellen; und

e) andere einschlägige Behörden nach nationalem Recht.

(7) Nach Erhalt der Informationen gemäß Absatz 6 bewerten die EBA, die ESMA oder die EIOPA und die EZB in Abstimmung mit der ENISA und in Zusammenarbeit mit der jeweils zuständigen Behörde, ob der schwerwiegende IKT-bezogene Vorfall für die zuständigen Behörden in anderen Mitgliedstaaten von Belang ist. Im Anschluss an diese Bewertung benachrichtigen die EBA, die ESMA oder die EIOPA die jeweils zuständigen Behörden in anderen Mitgliedstaaten entsprechend. Die EZB unterrichtet die Mitglieder des Europäischen Systems der Zentralbanken über die für das Zahlungssystem relevanten Aspekte. Auf der Grundlage dieser Unterrichtung treffen die zuständigen Behörden gegebenenfalls alle für die unmittelbare Stabilität des Finanzsystems notwendigen Schutzvorkehrungen.

([37]) Verordnung (EU) Nr. 806/2014 des Europäischen Parlaments und des Rates vom 15. Juli 2014 zur Festlegung einheitlicher Vorschriften und eines einheitlichen Verfahrens für die Abwicklung von Kreditinstituten und bestimmten Wertpapierfirmen im Rahmen eines einheitlichen Abwicklungsmechanismus und eines einheitlichen Abwicklungsfonds sowie zur Änderung der Verordnung (EU) Nr. 1093/2010 (ABl. L 225 vom 30.7.2014, S. 1).

(8) Die von der ESMA gemäß Absatz 7 vorzunehmende Meldung berührt nicht die Verantwortung der zuständigen Behörde, die Einzelheiten des schwerwiegenden IKT-bezogenen Vorfalls umgehend an die einschlägige Behörde des Aufnahmemitgliedstaats weiterzuleiten, wenn ein Zentralverwahrer eine umfassende grenzüberschreitende Tätigkeit in dem Aufnahmemitgliedstaat ausübt, der schwerwiegende IKT-bezogene Vorfall wahrscheinlich schwerwiegende Folgen für die Finanzmärkte des Aufnahmemitgliedstaats hat und zwischen den zuständigen Behörden Kooperationsvereinbarungen in Bezug auf die Beaufsichtigung von Finanzunternehmen bestehen.

Artikel 20

Harmonisierung von Inhalt und Vorlagen von Meldungen

Die ESA erarbeiten über den Gemeinsamen Ausschuss und in Abstimmung mit der ENISA und der EZB

a) gemeinsame Entwürfe technischer Regulierungsstandards, um

   i) den Inhalt von Meldungen über schwerwiegende IKT-bezogene Vorfälle festzulegen, damit den in Artikel 18 Absatz 1 aufgeführten Kriterien Rechnung getragen wird und weitere Elemente einbezogen werden, wie z. B. Einzelheiten zur Feststellung der Relevanz der Meldungen für andere Mitgliedstaaten und die Frage, ob es sich dabei um einen schwerwiegenden zahlungsbezogenen Betriebs- oder Sicherheitsvorfall handelt;

   ii) die Fristen für die Erstmeldung und jede Meldung nach Artikel 19 Absatz 4 festzulegen;

   iii) den Inhalt der Meldung erheblicher Cyberbedrohungen festzulegen.

   Bei der Ausarbeitung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte, um insbesondere sicherzustellen, dass den Besonderheiten der Finanzsektoren für die Zwecke des vorliegenden Absatzes Buchstabe a Ziffer ii gegebenenfalls durch unterschiedliche Fristen Rechnung getragen wird, unbeschadet der Beibehaltung eines kohärenten Ansatzes für die Meldung IKT-bezogener Vorfälle gemäß dieser Verordnung und gemäß der Richtlinie (EU) 2022/2555. Die ESA legen — sofern zutreffend — eine Begründung vor, wenn sie von den im Rahmen jener Richtlinie verfolgten Ansätzen abweichen;

b) gemeinsame Entwürfe technischer Durchführungsstandards zur Festlegung von Standardformularen, Vorlagen und Verfahren für Finanzunternehmen zur Meldung eines schwerwiegenden IKT-bezogenen Vorfalls oder einer erheblichen Cyberbedrohung.

Die ESA übermitteln der Kommission die in Absatz 1 Buchstabe a genannten gemeinsamen Entwürfe technischer Regulierungsstandards und die in Absatz 1 Buchstabe b genannten gemeinsamen Entwürfe technischer Durchführungsstandards bis zum 17. Juli 2024.

Der Kommission wird die Befugnis übertragen, diese Verordnung durch Annahme der in Absatz 1 Buchstabe a genannten gemeinsamen technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Der Kommission wird die Befugnis übertragen, die in Absatz 1 Buchstabe b genannten gemeinsamen technischen Durchführungsstandards gemäß Artikel 15 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 (EU) Nr. 1095/2010 zu erlassen.

Artikel 21

Zentralisierung der Berichterstattung über schwerwiegende IKT-bezogene Vorfälle

(1) Die ESA erstellen über den Gemeinsamen Ausschuss und in Abstimmung mit der EZB und der ENISA einen gemeinsamen Bericht, in dem sie die Durchführbarkeit einer weiteren Zentralisierung der Meldung von Vorfällen durch die Einrichtung einer einheitlichen EU-Plattform für die Meldung schwerwiegender IKT-bezogener Vorfälle durch Finanzunternehmen bewerten. In dem gemeinsamen Bericht werden Möglichkeiten sondiert, um den Meldefluss zu IKT-bezogenen Vorfällen zu erleichtern, damit verbundene Kosten zu senken und thematische Analysen zur Erhöhung aufsichtlicher Konvergenz zu unterstützen.

(2) Der in Absatz 1 genannte gemeinsame Bericht umfasst mindestens die folgenden Aspekte:

a) Voraussetzungen für die Einrichtung einer einheitlichen EU-Plattform;

b) Vorteile, Grenzen und Risiken, einschließlich Risiken im Zusammenhang mit einer hohen Konzentration sensibler Informationen;

c) die erforderliche Fähigkeit zur Gewährleistung der Interoperabilität im Hinblick auf andere einschlägige Meldesysteme;

d) Elemente des Betriebsmanagements;

e) Voraussetzungen für die Mitgliedschaft;

f) technische Regelungen für den Zugang von Finanzunternehmen und zuständigen nationalen Behörden zur einheitlichen EU-Plattform;

g) eine vorläufige Bewertung der finanziellen Kosten, die durch die Einrichtung der operativen Plattform zur Unterstützung der einheitlichen EU-Plattform entstehen, einschließlich des erforderlichen Fachwissens.

(3) Die ESA übermitteln dem Europäischen Parlament, dem Rat und der Kommission den in Absatz 1 genannten Bericht bis zum 17. Januar 2025.

Artikel 22

Rückmeldungen von Aufsichtsbehörden

(1) Unbeschadet der technischen Informationen, Empfehlungen oder Abhilfe- und Folgemaßnahmen, die im Einklang mit dem nationalen Recht gegebenenfalls vom CSIRT gemäß Richtlinie (EU) 2022/2555 bereitgestellt werden können, bestätigt die zuständige Behörde nach Eingang der Erstmeldung und jeder Meldung nach Artikel 19 Absatz 4 den Eingang und kann, wenn möglich, dem Finanzunternehmen zeitnah sachdienliche und angemessene Rückmeldungen oder allgemein gehaltene Orientierungshilfen übermitteln, insbesondere durch Zurverfügungstellung relevanter anonymisierter Informationen und Erkenntnisse zu ähnlichen Bedrohungen, sowie auf Ebene des Unternehmens angewandte Abhilfemaßnahmen und Möglichkeiten zur Minimierung und Minderung nachteiliger Auswirkungen auf den gesamten Finanzsektor erörtern. Unbeschadet der aufsichtlichen Rückmeldung bleiben Finanzunternehmen in vollem Umfang für die Handhabung und die Folgen der gemäß Artikel 19 Absatz 1 gemeldeten IKT-bezogenen Vorfälle verantwortlich.

(2) Die ESA berichten jährlich über den Gemeinsamen Ausschuss in anonymisierter und aggregierter Form über schwerwiegende IKT-bezogene Vorfälle, deren Einzelheiten von den zuständigen Behörden gemäß Artikel 19 Absatz 6 übermittelt werden, und geben dabei mindestens die Zahl schwerwiegender IKT-bezogener Vorfälle, ihre Art und ihre Auswirkungen auf die Geschäftstätigkeit von Finanzunternehmen oder Kunden sowie die ergriffenen Abhilfemaßnahmen und die Kosten an.

Die ESA geben Warnungen heraus und erstellen allgemein gehaltene Statistiken, um die Bewertungen von Bedrohungen und Schwachstellen im IKT-Bereich zu unterstützen.

Artikel 23

Zahlungsbezogene Betriebs- oder Sicherheitsvorfälle, die Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister und E-Geld-Institute betreffen

Die Anforderungen in diesem Kapitel gelten auch für zahlungsbezogene Betriebs- oder Sicherheitsvorfälle, auch schwerwiegender Art, wenn sie Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister und E-Geld-Institute betreffen.

KAPITEL IV

Testen der digitalen operationalen Resilienz

Artikel 24

Allgemeine Anforderungen für das Testen der digitalen operationalen Resilienz

(1) Um die Vorbereitung auf die Handhabung IKT-bezogener Vorfälle zu bewerten, Schwächen, Mängel und Lücken in Bezug auf die digitale operationale Resilienz zu erkennen und Korrekturmaßnahmen umgehend umzusetzen, erstellen, pflegen und überprüfen Finanzunternehmen, die keine Kleinstunternehmen sind, unter Berücksichtigung der in Artikel 4 Absatz 2 aufgeführten Kriterien ein solides und umfassendes Programm für das Testen der digitalen operationalen Resilienz als integraler Bestandteil des in Artikel 6 genannten IKT-Risikomanagementrahmens.

(2) Das Programm für Tests der digitalen operationalen Resilienz umfasst eine Reihe von Bewertungen, Tests, Methoden, Verfahren und Tools, die gemäß den Artikeln 25 und 26 anzuwenden sind.

(3) Bei der Ausführung des in Absatz 1 genannten Programms für das Testen der digitalen operationalen Resilienz wenden Finanzunternehmen, die keine Kleinstunternehmen sind, unter Berücksichtigung der in Artikel 4 Absatz 2 aufgeführten Kriterien einen risikobasierten Ansatz an, wobei sie die sich entwickelnden IKT-Risikolandschaften, etwaige spezifische Risiken, denen das betreffende Finanzunternehmen ausgesetzt ist oder ausgesetzt sein könnte, die Kritikalität von Informationsassets und erbrachten Dienstleistungen sowie alle sonstigen Faktoren, die das Finanzunternehmen für angemessen hält, gebührend berücksichtigen.

(4) Finanzunternehmen, die keine Kleinstunternehmen sind, stellen sicher, dass Tests von unabhängigen, internen oder externen Parteien durchgeführt werden. Werden die Tests von einem internen Tester durchgeführt, stellen die Finanzunternehmen ausreichende Ressourcen bereit und tragen dafür Sorge, dass während der Konzeptions- und Durchführungsphase der Prüfung keine Interessenkonflikte entstehen.

(5) Finanzunternehmen, die keine Kleinstunternehmen sind, legen Verfahren und Leitlinien zur Priorisierung, Klassifizierung und Behebung aller während der Durchführung der Tests zutage getretenen Probleme fest und legen interne Validierungsmethoden fest, um sicherzustellen, dass alle ermittelten Schwächen, Mängel oder Lücken vollständig angegangen werden.

(6) Finanzunternehmen, die keine Kleinstunternehmen sind, stellen sicher, dass bei allen IKT-Systemen und -Anwendungen, die kritische oder wichtige Funktionen unterstützen, mindestens einmal jährlich angemessene Tests durchgeführt werden.

Artikel 25

Testen von IKT-Tools und -Systemen

(1) Das in Artikel 24 genannte Programm für die Tests der digitalen operationalen Resilienz beinhaltet im Einklang mit den in Artikel 4 Absatz 2 aufgeführten Kriterien die Durchführung angemessener Tests, wie etwa Schwachstellenbewertung und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests.

(2) Zentralverwahrer und zentrale Gegenparteien führen Schwachstellenbewertungen durch, bevor Anwendungen und Infrastrukturkomponenten sowie IKT-Dienstleistungen, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen, eingesetzt oder wieder eingesetzt werden.

(3) Kleinstunternehmen führen die in Absatz 1 genannten Tests durch, indem sie einen risikobasierten Ansatz mit einer strategischen Planung für IKT-Tests kombinieren, wobei sie gebührend berücksichtigen, dass zwischen dem Umfang von Ressourcen und der Zeit, die für die IKT-Tests gemäß diesem Artikel aufzuwenden sind, einerseits, und der Dringlichkeit, der Art des Risikos, der Kritikalität von Informationsassets und erbrachten Dienstleistungen sowie allen sonstigen relevanten Faktoren, einschließlich der Fähigkeit des Finanzunternehmens, kalkulierte Risiken einzugehen, andererseits, ein ausgewogenes Verhältnis gewahrt werden muss.

Artikel 26

Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT

(1) Gemäß Absatz 8 Unterabsatz 3 des vorliegenden Artikels ermittelte Finanzunternehmen, bei denen es sich weder um die in Artikel 16 Absatz 1 Unterabsatz 1 genannten Unternehmen noch um Kleinstunternehmen handelt, führen mindestens alle drei Jahre anhand von TLPT erweiterte Tests durch. Auf der Grundlage des Risikoprofils des Finanzunternehmens und unter Berücksichtigung der betrieblichen Gegebenheiten kann die zuständige Behörde das Finanzunternehmen erforderlichenfalls auffordern, die Häufigkeit dieser Tests zu verringern oder zu erhöhen.

(2) Jeder bedrohungsorientierte Penetrationstest schließt mehrere oder alle kritischen oder wichtigen Funktionen eines Finanzunternehmens ein und wird an Live-Produktionssystemen durchgeführt, die derartige Funktionen unterstützen.

Finanzunternehmen ermitteln alle relevanten zugrunde liegenden IKT-Systeme, -Prozesse und -Technologien, die kritische oder wichtige Funktionen und IKT-Dienstleistungen unterstützen, einschließlich derer, die diejenigen kritischen oder wichtigen Funktionen unterstützen, die an IKT-Drittdienstleister ausgelagert oder per Vertrag vergeben wurden.

Finanzunternehmen bewerten, welche kritischen oder wichtigen Funktionen ein TLPT einschließen muss. Der genaue Umfang von TLPT ist vom Ergebnis dieser Bewertung abhängig und wird von den zuständigen Behörden validiert.

(3) Sind IKT-Drittdienstleister in das Spektrum der TLPT einbezogen, ergreift das Finanzunternehmen alle erforderlichen Maßnahmen und Vorkehrungen, um die Einbindung dieser IKT-Drittdienstleister in die TLPT sicherzustellen, und trägt jederzeit die volle Verantwortung für die Gewährleistung der Einhaltung dieser Verordnung.

(4) Wenn vernünftigerweise davon auszugehen ist, dass sich die Einbindung eines IKT-Drittdienstleisters in einen TLPT gemäß Absatz 3 nachteilig auf die Qualität oder die Sicherheit von Dienstleistungen des IKT-Drittdienstleisters an Kunden, bei denen es sich um nicht in den Anwendungsbereich dieser Verordnung fallende Unternehmen handelt, oder auf die Vertraulichkeit in Bezug auf die mit diesen Dienstleistungen verbundenen Daten auswirkt, können das Finanzunternehmen und der IKT-Drittdienstleister unbeschadet Absatz 2 Unterabsätze 1 und 2 schriftlich vereinbaren, dass der IKT-Drittdienstleister unmittelbar vertragliche Vereinbarungen mit einem externen Tester schließt, um unter der Leitung eines benannten Finanzunternehmens einen gebündelten TLPT durchzuführen, an dem mehrere Finanzunternehmen beteiligt sind (gebündelter Test), für die der IKT-Drittdienstleister IKT-Dienstleistungen erbringt.

Diese gebündelten Tests erstrecken sich auf das relevante Spektrum von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von den Finanzunternehmen per Vertrag an die jeweiligen IKT-Drittdienstleister vergeben wurden. Die gebündelten Tests gelten als TLPT, die von den an den gebündelten Tests beteiligten Finanzunternehmen durchgeführt werden.

Die Zahl der Finanzunternehmen, die sich an den gebündelten Tests beteiligen, wird unter Berücksichtigung der Komplexität und der Art der betreffenden Dienstleistungen angemessen austariert.

(5) Finanzunternehmen wenden in Zusammenarbeit mit IKT-Drittdienstleistern und anderen beteiligten Parteien, einschließlich der Tester, jedoch ohne die zuständigen Behörden, wirksame Risikomanagementkontrollen an, um die Gefahr von potenziellen Auswirkungen auf Daten, Schäden an Vermögenswerten und Unterbrechungen kritischer oder wichtiger Funktionen, Dienste oder Vorgänge im Finanzunternehmen selbst, seinen Gegenparteien oder im Finanzsektor zu mindern.

(6) Nach Abschluss der Tests und der Ausarbeitung von Berichten und Plänen mit Abhilfemaßnahmen legen das Finanzunternehmen und gegebenenfalls die externen Tester der gemäß Absatz 9 oder 10 benannten Behörde eine Zusammenfassung der maßgeblichen Ergebnisse, die Pläne mit Abhilfemaßnahmen und die Unterlagen vor, mit denen belegt wird, dass der TLPT anforderungsgemäß durchgeführt wurden.

(7) Die Behörden stellen Finanzunternehmen eine Bescheinigung aus, aus der hervorgeht, dass der Test — wie in den Unterlagen nachgewiesen — im Einklang mit den Anforderungen durchgeführt wurde, um die gegenseitige Anerkennung bedrohungsorientierter Penetrationstests zwischen den zuständigen Behörden zu ermöglichen. Das Finanzunternehmen übermittelt der jeweils zuständigen Behörde die Bescheinigung, die Zusammenfassung der maßgeblichen Ergebnisse und die Abhilfemaßnahmen.

Unbeschadet einer solchen Bescheinigung bleiben Finanzunternehmen jederzeit in vollem Umfang für die Auswirkungen der in Absatz 4 genannten Tests verantwortlich.

(8) Finanzunternehmen beauftragen Tester für die Zwecke der Durchführung von TLPT gemäß Artikel 27. Ziehen Finanzunternehmen für die Zwecke der Durchführung von TLPT interne Tester heran, so beauftragen sie für jeden dritten Test einen externen Tester.

Kreditinstitute, die gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 als bedeutend eingestuft wurden, ziehen nur externe Tester gemäß Artikel 27 Absatz 1 Buchstaben a bis e heran.

Die zuständigen Behörden ermitteln Finanzunternehmen, die TLPT durchzuführen haben, unter Berücksichtigung der in Artikel 4 Absatz 2 aufgeführten Kriterien und stützen sich dabei auf die Bewertung von:

a) wirkungsbezogenen Faktoren, darunter insbesondere inwieweit sich die vom Finanzunternehmen erbrachten Dienstleistungen und ausgeführten Tätigkeiten auf den Finanzsektor auswirken;

b) etwaigen Bedenken hinsichtlich der Finanzstabilität, einschließlich des systemischen Charakters des Finanzunternehmens auf Unionsebene oder auf nationaler Ebene, je nach Sachlage;

c) dem spezifischen IKT-Risikoprofil, dem IKT-Reifegrad des Finanzunternehmens oder einschlägigen technologischen Merkmalen.

(9) Die Mitgliedstaaten können eine einzige staatliche Behörde für den Finanzsektor benennen, die auf nationaler Ebene für mit TLPT verbundenen Angelegenheiten im Finanzsektor zuständig ist, und betrauen sie mit allen diesbezüglichen Zuständigkeiten und Aufgaben.

(10) In Ermangelung einer Benennung gemäß Absatz 9 und unbeschadet der Befugnis zur Ermittlung der Finanzunternehmen, die verpflichtet sind, TLPT durchzuführen, kann eine zuständige Behörde die Wahrnehmung einiger oder aller in diesem Artikel oder in Artikel 27 genannten Aufgaben auf eine andere für den Finanzsektor zuständige nationale Behörde übertragen.

(11) Die ESA arbeiten im Einvernehmen mit der EZB im Einklang mit dem TIBER-EU-Rahmen gemeinsame Entwürfe technischer Regulierungsstandards aus, in denen Folgendes präzisiert wird:

a) die für die Zwecke der Anwendung von Absatz 8 Unterabsatz 2 herangezogenen Kriterien;

b) die Anforderungen und Standards für den Einsatz interner Tester;

c) die Anforderungen hinsichtlich:

   i) des Umfangs der in Absatz 2 genannten TLPT;

   ii) der Testmethodik und des Testkonzepts für jede einzelne Phase des Testverfahrens;

   iii) der Ergebnisse, des Abschlusses und der Behebungsphasen der Tests;

d) der Art der aufsichtlichen und sonstigen relevanten Zusammenarbeit, die für die Umsetzung von TLPT und die Erleichterung der gegenseitigen Anerkennung dieser Tests im Kontext von Finanzunternehmen, die in mehr als einem Mitgliedstaat tätig sind, erforderlich ist, um eine angemessene Beteiligung der Aufsichtsbehörden und eine flexible Umsetzung zu ermöglichen, damit den Besonderheiten finanzieller Teilsektoren oder lokaler Finanzmärkte Rechnung getragen wird.

Bei der Ausarbeitung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA gebührend etwaige Besonderheiten, die sich aus der unterschiedlichen Art der Tätigkeiten in verschiedenen Finanzdienstleistungssektoren ergeben.

Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Juli 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Artikel 27

Anforderungen an Tester bezüglich der Durchführung von TLPT

(1) Finanzunternehmen ziehen für TLPT nur Tester heran, die

a) von höchster Eignung und Ansehen sind;

b) über technische und organisatorische Fähigkeiten verfügen und spezifisches Fachwissen in den Bereichen Bedrohungsanalyse, Penetrationstests und Red-Team-Tests nachweisen;

c) von einer Akkreditierungsstelle in einem Mitgliedstaat zertifiziert wurden oder formale Verhaltenskodizes oder ethische Rahmenregelungen einhalten;

d) eine unabhängige Gewähr oder einen Auditbericht in Bezug auf das zuverlässige Management von Risiken vorlegen, die mit der Durchführung von TLPT verbunden sind, darunter auch der angemessene Schutz vertraulicher Informationen des Finanzunternehmens und ein Ausgleich der geschäftlichen Risiken des Finanzunternehmens;

e) ordnungsgemäß und vollständig durch einschlägige Berufshaftpflichtversicherungen abgesichert sind, einschließlich einer Versicherung gegen das Risiko von Fehlverhalten und Fahrlässigkeit.

(2) Beim Einsatz interner Tester gewährleisten Finanzunternehmen, dass neben den Anforderungen in Absatz 1 auch folgende Bedingungen erfüllt sind:

a) der Einsatz wurde von der jeweils zuständigen Behörde oder von der gemäß Artikel 26 Absätze 9 und 10 benannten einzigen staatlichen Behörde genehmigt;

b) die jeweils zuständige Behörde hat überprüft, dass das Finanzunternehmen über ausreichende Ressourcen verfügt und sichergestellt hat, dass während der Konzeptions- und Durchführungsphase der Tests keine Interessenkonflikte entstehen; und

c) der Anbieter von Bedrohungsanalysen gehört nicht dem Finanzunternehmen an.

(3) Finanzunternehmen stellen sicher, dass in Verträgen, die mit externen Testern geschlossen werden, eine ordentliche Handhabung der Ergebnisse von TLPT vorgesehen ist und die diesbezügliche Datenverarbeitung, einschließlich Generierung, Speicherung, Aggregation, Entwurf, Berichterstattung, Weitergabe oder Vernichtung, keine Risiken für das Finanzunternehmen mit sich bringt.

KAPITEL V

Management des IKT-Drittparteienrisikos

Abschnitt I

Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos

Artikel 28

Allgemeine Prinzipien

(1) Finanzunternehmen managen das IKT-Drittparteienrisiko als integralen Bestandteil des IKT-Risikos innerhalb ihres IKT-Risikomanagementrahmens nach Artikel 6 Absatz 1 und im Einklang mit den folgenden Prinzipien:

a) Finanzunternehmen, die vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen für die Ausübung ihrer Geschäftstätigkeit getroffen haben, bleiben jederzeit in vollem Umfang für die Einhaltung und Erfüllung aller Verpflichtungen nach dieser Verordnung und nach dem anwendbaren Finanzdienstleistungsrecht verantwortlich.

b) Beim Management des IKT-Drittparteienrisikos tragen Finanzunternehmen dem Grundsatz der Verhältnismäßigkeit Rechnung, wobei Folgendes zu berücksichtigen ist:

i) die Art, das Ausmaß, die Komplexität und die Relevanz IKT-bezogener Abhängigkeiten,

ii) die Risiken infolge vertraglicher Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die mit IKT-Drittdienstleistern geschlossen wurden, wobei die Kritikalität oder Relevanz der jeweiligen Dienstleistungen, Prozesse oder Funktionen sowie die potenziellen Auswirkungen auf die Kontinuität und Verfügbarkeit von Finanzdienstleistungen und -tätigkeiten auf Einzel- und Gruppenebene zu berücksichtigen sind.

(2) Finanzinstitute, bei denen es sich weder um die in Artikel 16 Absatz 1 Unterabsatz 1 genannten Unternehmen noch um Kleinstunternehmen handelt, beschließen im Rahmen ihres IKT-Risikomanagementrahmens eine Strategie für das IKT-Drittparteienrisiko und überprüfen diese regelmäßig, wobei gegebenenfalls die in Artikel 6 Absatz 9 genannte Strategie zur Nutzung mehrerer Anbieter Berücksichtigung findet. Die Strategie zum IKT-Drittparteienrisiko umfasst eine Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden, und gilt auf individueller und gegebenenfalls teilkonsolidierter und konsolidierter Basis. Das Leitungsorgan überprüft auf der Grundlage einer Bewertung des Gesamtrisikoprofils des Finanzunternehmens und des Umfangs und der Komplexität der Unternehmensdienstleistungen regelmäßig Risiken, die im Zusammenhang mit den vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen ermittelt werden.

(3) Finanzunternehmen führen und aktualisieren im Rahmen ihres IKT-Risikomanagementrahmens auf Unternehmensebene sowie auf teilkonsolidierter und konsolidierter Ebene ein Informationsregister, das sich auf alle vertraglichen Vereinbarungen über die Nutzung von durch IKT-Drittdienstleister bereitgestellten IKT-Dienstleistungen bezieht.

Die vertraglichen Vereinbarungen gemäß Unterabsatz 1 werden angemessen dokumentiert, wobei zwischen Vereinbarungen, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen abdecken, und solchen unterschieden wird, bei denen dies nicht der Fall ist.

Finanzunternehmen erstatten den zuständigen Behörden mindestens einmal jährlich Bericht zur Anzahl neuer Vereinbarungen über die Nutzung von IKT-Dienstleistungen, den Kategorien von IKT-Drittdienstleistern, der Art der vertraglichen Vereinbarungen sowie den bereitgestellten IKT-Dienstleistungen und -Funktionen.

Finanzunternehmen stellen der zuständigen Behörde auf Verlangen das vollständige Informationsregister oder auf Anfrage bestimmte Teile dieses Registers zusammen mit allen Informationen zur Verfügung, die für eine wirksame Beaufsichtigung des Finanzunternehmens als notwendig erachtet werden.

Finanzunternehmen unterrichten die zuständige Behörde zeitnah über jede geplante vertragliche Vereinbarung über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sowie in dem Fall, dass eine Funktion kritisch oder wichtig geworden ist.

(4) Vor Abschluss einer vertraglichen Vereinbarung über die Nutzung von IKT-Dienstleistungen müssen Finanzunternehmen:

a) beurteilen, ob sich die vertragliche Vereinbarung auf die Nutzung von IKT-Dienstleistungen zur Unterstützung einer kritischen oder wichtigen Funktion bezieht;

b) beurteilen, ob die aufsichtsrechtlichen Bedingungen für die Auftragsvergabe erfüllt sind;

c) alle relevanten Risiken im Zusammenhang mit der vertraglichen Vereinbarung ermitteln und bewerten, einschließlich der Möglichkeit, dass diese vertragliche Vereinbarung dazu beitragen kann, das in Artikel 29 genannte IKT-Konzentrationsrisiko zu erhöhen;

d) bei potenziellen IKT-Drittdienstleistern der gebotenen Sorgfaltspflicht nachkommen und während des gesamten Auswahl- und Bewertungsprozesses sicherstellen, dass der IKT-Drittdienstleister geeignet ist;

e) Interessenkonflikte, die durch die vertragliche Vereinbarung entstehen können, ermitteln und bewerten.

(5) Finanzunternehmen dürfen vertragliche Vereinbarungen nur mit IKT-Drittdienstleistern schließen, die angemessene Standards für Informationssicherheit einhalten. Betreffen diese vertraglichen Vereinbarungen kritische oder wichtige Funktionen, so berücksichtigen die Finanzunternehmen vor Abschluss der Vereinbarungen angemessen, ob die IKT-Drittdienstleister die aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit anwenden.

(6) Bei der Ausübung der Zugangs-, Inspektions- und Auditrechte in Bezug auf den IKT-Drittdienstleister bestimmen Finanzunternehmen auf der Grundlage eines risikobasierten Ansatzes vorab die Häufigkeit von Audits und Inspektionen sowie die zu prüfenden Bereiche, indem allgemein anerkannte Auditstandards im Einklang mit etwaigen Aufsichtsanweisungen für die Anwendung und Einbeziehung solcher Auditstandards eingehalten werden.

Wenn vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die mit IKT-Drittdienstleistern geschlossen werden, ein hohes Maß an technischer Komplexität mit sich bringen, überprüft das Finanzunternehmen, dass die internen oder externen Revisoren oder ein Revisorenpool über die Fähigkeiten und Kenntnisse verfügen bzw. verfügt, die für die wirksame Durchführung der einschlägigen Audits und Bewertungen erforderlich sind.

(7) Finanzunternehmen stellen sicher, dass vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen gekündigt werden können, wenn einer der folgenden Umstände vorliegt:

a) ein erheblicher Verstoß des IKT-Drittdienstleisters gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen;

b) Umstände, die im Laufe der Überwachung des IKT-Drittparteienrisikos festgestellt wurden und die als geeignet eingeschätzt werden, die Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen zu beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des IKT-Drittdienstleisters auswirken;

c) nachweisliche Schwächen des IKT-Drittdienstleisters in Bezug auf sein allgemeines IKT-Risikomanagement und insbesondere bei der Art und Weise, in der er die Verfügbarkeit, Authentizität, Sicherheit und Vertraulichkeit von Daten gewährleistet, unabhängig davon, ob es sich um personenbezogene oder anderweitig sensible Daten oder nicht personenbezogene Daten handelt;

d) die zuständige Behörde kann das Finanzunternehmen infolge der Bedingungen der jeweiligen vertraglichen Vereinbarung oder der mit dieser Vereinbarung verbundenen Umstände nicht mehr wirksam beaufsichtigen.

(8) Für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, richten Finanzunternehmen Ausstiegsstrategien ein. In den Ausstiegsstrategien wird den Risiken Rechnung getragen, die auf der Ebene der IKT-Drittdienstleister entstehen können, darunter insbesondere ein möglicher Fehler des IKT-Drittdienstleisters, eine Verschlechterung der Qualität der bereitgestellten IKT-Dienstleistungen, jede Unterbrechung der Geschäftstätigkeit aufgrund unangemessener oder unterlassener Bereitstellung von IKT-Dienstleistungen oder jedes erhebliche Risiko im Zusammenhang mit der angemessenen und kontinuierlichen Bereitstellung der jeweiligen IKT-Dienstleistungen oder der Beendigung vertraglicher Vereinbarungen mit IKT-Drittdienstleistern unter einem der in Absatz 7 genannten Umstände.

Finanzunternehmen stellen sicher, dass sie aus vertraglichen Vereinbarungen ausscheiden können, ohne:

a) Unterbrechung ihrer Geschäftstätigkeit,

b) Einschränkung der Einhaltung regulatorischer Anforderungen,

c) Beeinträchtigung der Kontinuität und Qualität ihrer für Kunden erbrachten Dienstleistungen.

Ausstiegspläne müssen umfassend, dokumentiert und im Einklang mit den in Artikel 4 Absatz 2 aufgeführten Kriterien ausreichend getestet sein sowie regelmäßig überprüft werden.

Finanzunternehmen ermitteln alternative Lösungen und entwickeln Übergangspläne, die es ihnen ermöglichen, dem IKT-Drittdienstleister die vertraglich vereinbarten IKT-Dienstleistungen und die relevanten Daten zu entziehen und sie sicher und vollständig alternativen Anbietern zu übertragen oder wieder in die eigenen Systeme zu überführen.

Finanzunternehmen verfügen über angemessene Notfallmaßnahmen, um die Fortführung der Geschäftstätigkeit zu gewährleisten, falls die in Unterabsatz 1 genannten Umstände auftreten.

(9) Die ESA erarbeiten über den Gemeinsamen Ausschuss Entwürfe technischer Durchführungsstandards, um die Standardvorlagen für die Zwecke des in Absatz 3 genannten Informationsregisters festzulegen, einschließlich Informationen, die allen vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen gemein sind. Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, die in Unterabsatz 1 genannten technischen Durchführungsstandards gemäß Artikel 15 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu erlassen.

(10) Die ESA erarbeiten über den Gemeinsamen Ausschuss Entwürfe für technische Regulierungsstandards, um den detaillierten Inhalt der Leitlinie, die in Absatz 2 in Bezug auf die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer und wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden, genannt wird, weiter zu spezifizieren.

Bei der Ausarbeitung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte. Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Artikel 29

Vorläufige Bewertung des IKT-Konzentrationsrisikos auf Unternehmensebene

(1) Bei der Ermittlung und Bewertung der in Artikel 28 Absatz 4 Buchstabe c genannten Risiken berücksichtigen Finanzunternehmen zudem, ob der geplante Abschluss einer vertraglichen Vereinbarung in Bezug auf IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, Folgendes herbeiführen würde:

a) Verträge mit einem IKT-Drittdienstleister, der nicht ohne Weiteres ersetzbar ist; oder

b) mehrfache vertragliche Vereinbarungen über die Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen mit demselben IKT-Drittdienstleister oder mit eng verbundenen IKT-Drittdienstleistern.

Finanzunternehmen wägen Nutzen und Kosten alternativer Lösungen ab, z. B. die Nutzung verschiedener IKT-Drittdienstleister, und berücksichtigen, ob und wie geplante Lösungen den geschäftlichen Erfordernissen und Zielen entsprechen, die in ihrer Strategie für digitale Resilienz festgelegt sind.

(2) Ist in der vertraglichen Vereinbarung über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen die Möglichkeit vorgesehen, dass ein IKT-Drittdienstleister IKT-Dienstleistungen zur Unterstützung einer kritischen oder wichtigen Funktion per Unterauftrag an andere IKT-Drittdienstleister vergibt, wägen Finanzunternehmen die Vorteile und Risiken ab, die im Zusammenhang mit einer solchen Unterauftragsvergabe entstehen können, insbesondere sofern der IKT-Unterauftragnehmer in einem Drittland niedergelassen ist.

Betreffen vertragliche Vereinbarungen IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, berücksichtigen die Finanzunternehmen gebührend die Bestimmungen des Insolvenzrechts, die im Falle der Insolvenz des IKT-Drittdienstleisters anwendbar wären, sowie jede Einschränkung, die sich im Zusammenhang mit der dringenden Wiederherstellung der Daten des Finanzunternehmens ergeben könnte.

Werden mit einem IKT-Drittdienstleister mit Sitz in einem Drittland vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen geschlossen, so beachten Finanzunternehmen neben den in Unterabsatz 2 genannten Umständen auch, dass die Datenschutzvorschriften der Union eingehalten und die Rechtsvorschriften in diesem Drittland wirksam durchgesetzt werden.

Ist in den vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen die Unterauftragsvergabe vorgesehen, so bewerten die Finanzunternehmen, ob und wie sich potenziell lange oder komplexe Ketten der Unterauftragsvergabe auf ihre Fähigkeit auswirken können, die vertraglich vereinbarten Funktionen vollständig zu überwachen, und ob die zuständige Behörde in dieser Hinsicht in der Lage ist, das Finanzunternehmen wirksam zu beaufsichtigen.

Artikel 30

Wesentliche Vertragsbestimmungen

(1) Die Rechte und Pflichten des Finanzunternehmens und des IKT-Drittdienstleisters werden eindeutig zugewiesen und schriftlich dargelegt. Der vollständige Vertrag umfasst die Vereinbarung über die Dienstleistungsgüte und wird in einem schriftlichen Dokument, das den Parteien in Papierform zur Verfügung steht, oder in einem Dokument in einem anderen herunterladbaren, dauerhaften und zugänglichen Format dokumentiert.

(2) Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente:

a) eine klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen, die der IKT-Drittdienstleister bereitzustellen hat, wobei anzugeben ist, ob die Vergabe von Unteraufträgen für IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, zulässig ist, und — wenn dies der Fall ist — welche Bedingungen für diese Unterauftragsvergabe gelten;

b) die Standorte — das heißt die Regionen oder Länder —, an denen die vertraglich vereinbarten oder an Unterauftragnehmer vergebenen Funktionen und IKT-Dienstleistungen bereitzustellen sind und an denen Daten verarbeitet werden sollen, einschließlich des Speicherorts, sowie die Auflage für den IKT-Drittdienstleister, das Finanzunternehmen vorab zu benachrichtigen, wenn er eine Änderung dieser Standorte beabsichtigt;

c) Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz, einschließlich des Schutzes personenbezogener Daten;

d) Bestimmungen über die Sicherstellung des Zugangs zu personenbezogenen und nicht personenbezogenen Daten, die von dem Finanzunternehmen im Fall einer Insolvenz, Abwicklung, Einstellung der Geschäftstätigkeit des IKT-Drittdienstleisters oder einer Beendigung der vertraglichen Vereinbarungen verarbeitet werden, sowie über die Wiederherstellung und Rückgabe dieser Daten in einem leicht zugänglichen Format;

e) Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen;

f) die Verpflichtung des IKT-Drittdienstleisters, dem Finanzunternehmen bei einem IKT-Vorfall, der mit dem für das Finanzunternehmen bereitgestellten IKT-Dienst in Verbindung steht, ohne zusätzliche Kosten oder zu vorab festzusetzenden Kosten Unterstützung zu leisten;

g) die Verpflichtung des IKT-Drittdienstleisters, vollumfänglich mit den für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden zusammenzuarbeiten, einschließlich der von diesen benannten Personen;

h) Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechend den Erwartungen der zuständigen Behörden und der Abwicklungsbehörden;

i) Bedingungen für die Teilnahme von IKT-Drittdienstleistern an den von den Finanzunternehmen angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz gemäß Artikel 13 Absatz 6.

(3) Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes:

a) vollständige Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen, mit präzisen quantitativen und qualitativen Leistungszielen innerhalb der vereinbarten Dienstleistungsgüte, um dem Finanzunternehmen eine wirksame Überwachung von IKT-Dienstleistungen und das unverzügliche Ergreifen angemessener Korrekturmaßnahmen zu ermöglichen, wenn eine vereinbarte Dienstleistungsgüte nicht erreicht wird;

b) Kündigungsfristen und Berichtspflichten des IKT-Drittdienstleisters gegenüber dem Finanzunternehmen, einschließlich der Meldung aller Entwicklungen, die sich wesentlich auf die Fähigkeit des IKT-Drittdienstleisters, IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen gemäß den vereinbarten Leistungsniveaus wirksam bereitzustellen, auswirken könnten;

c) Anforderungen an den IKT-Drittdienstleister, Notfallpläne zu implementieren und zu testen und über Maßnahmen, Tools und Leit- und Richtlinien für IKT-Sicherheit zu verfügen, die ein angemessenes Maß an Sicherheit für die Erbringung von Dienstleistungen durch das Finanzunternehmen im Einklang mit seinem Rechtsrahmen bieten;

d) die Verpflichtung des IKT-Drittdienstleisters, sich an den in den Artikeln 26 und 27 genannten TLPT des Finanzunternehmens zu beteiligen und uneingeschränkt daran mitzuwirken;

e) das Recht, die Leistung des IKT-Drittdienstleisters fortlaufend zu überwachen, wozu Folgendes gehört:

i) uneingeschränkte Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens oder eines beauftragten Dritten und der zuständigen Behörde sowie das Recht auf Anfertigung von Kopien einschlägiger Unterlagen vor Ort, wenn ihnen für die Geschäftstätigkeit des IKT-Drittdienstleisters entscheidende Bedeutung zukommt, wobei die tatsächliche Ausübung dieser Rechte nicht durch andere vertragliche Vereinbarungen oder Umsetzungsrichtlinien behindert oder eingeschränkt wird;

ii) das Recht, alternative Bestätigungsniveaus zu vereinbaren, wenn die Rechte anderer Kunden betroffen sind;

iii) die Verpflichtung des IKT-Drittdienstleisters zur uneingeschränkten Zusammenarbeit bei Vor-Ort-Inspektionen und Audits, die von den zuständigen Behörden, der federführenden Überwachungsbehörde, dem Finanzunternehmen oder einem beauftragten Dritten durchgeführt werden; und

iv) die Verpflichtung, Einzelheiten zu Umfang und Häufigkeit dieser Inspektionen sowie dem dabei zu befolgenden Verfahren mitzuteilen;

f) Ausstiegsstrategien, insbesondere die Festlegung eines verbindlichen angemessenen Übergangszeitraums,

i) in dem der IKT-Drittdienstleister weiterhin die entsprechenden Funktionen oder IKT-Dienstleistungen bereitstellt, um das Risiko von Störungen im Finanzunternehmen zu verringern oder um dessen geordnete Abwicklung und Umstrukturierung sicherzustellen;

ii) der dem Finanzunternehmen ermöglicht, zu einem anderen IKT-Drittdienstleister zu wechseln oder auf interne Lösungen umzustellen, die der Komplexität der erbrachten Dienstleistung entsprechen.

Abweichend von Buchstabe e können der IKT-Drittdienstleister und das Finanzunternehmen, das ein Kleinstunternehmen ist, vereinbaren, dass die Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens auf einen unabhängigen Dritten übertragen werden können, der vom IKT-Drittdienstleister benannt wird, sowie dass das Finanzunternehmen von diesem Dritten jederzeit Informationen und Gewähr in Bezug auf die Leistung des IKT-Drittdienstleisters verlangen kann.

(4) Bei der Aushandlung vertraglicher Vereinbarungen erwägen Finanzunternehmen und IKT-Drittdienstleister die Verwendung von Standardvertragsklauseln, die von Behörden für bestimmte Dienstleistungen entwickelt wurden.

(5) Die ESA erarbeiten über den Gemeinsamen Ausschuss Entwürfe technischer Regulierungsstandards, um die in Absatz 2 Buchstabe a genannten Aspekte zu präzisieren, die ein Finanzunternehmen bei der Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen bestimmen und bewerten muss.

Bei der Ausarbeitung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte.

Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Juli 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Abschnitt II

Überwachungsrahmen für kritische IKT-Drittdienstleister

Artikel 31

Einstufung kritischer IKT-Drittdienstleister

(1) Die ESA nehmen über den Gemeinsamen Ausschuss und auf Empfehlung des gemäß Artikel 32 Absatz 1 eingerichteten Überwachungsforums folgende Aufgaben wahr:

a) Einstufung der IKT-Drittdienstleister, die für Finanzunternehmen kritisch sind, nachdem eine entsprechende Bewertung unter Berücksichtigung der in Absatz 2 genannten Kriterien durchgeführt wurde;

b) Ernennung derjenigen Europäischen Aufsichtsbehörde zur federführenden Überwachungsbehörde für jeden kritischen IKT-Drittdienstleister, die gemäß den Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 bzw. (EU) Nr. 1095/2010 für diejenigen Finanzunternehmen zuständig ist, die nachweislich der Summe der einzelnen Bilanzen dieser Finanzunternehmen zusammen den größten Anteil des Gesamtvermögens am Gesamtwert der Aktiva aller Finanzunternehmen halten, die die Dienste des betreffenden kritischen IKT-Drittdienstleisters nutzen.

(2) Die Einstufung nach Absatz 1 Buchstabe a basiert in Bezug auf IKT-Dienstleistungen, die vom IKT-Drittdienstleister bereitgestellt werden, auf den folgenden Kriterien:

a) den systemischen Auswirkungen auf die Stabilität, Kontinuität oder Qualität der Erbringung von Finanzdienstleistungen, falls der betreffende IKT-Drittdienstleister bei der Erbringung seiner Dienste einer umfassenden Betriebsstörung ausgesetzt wäre, wobei die Zahl von Finanzunternehmen und der Gesamtwert der Aktiva derjenigen Finanzunternehmen zu berücksichtigen ist, für die der betreffende IKT-Drittdienstleister Dienstleistungen erbringt;

b) dem systemischen Charakter oder der Bedeutung der Finanzunternehmen, die auf den jeweiligen IKT-Drittdienstleister zurückgreifen, bewertet anhand der folgenden Parameter:

   i) der Anzahl global systemrelevanter Institute (G-SRI) oder anderer systemrelevanter Institute (A-SRI), die auf den jeweiligen IKT-Drittdienstleister zurückgreifen;

   ii) der Interdependenz zwischen den unter Ziffer i genannten G-SRI oder A-SRI und anderen Finanzunternehmen, einschließlich der Fälle, in denen die G-SRI oder A-SRI Finanzinfrastrukturdienstleistungen für andere Finanzunternehmen erbringen;

c) der Abhängigkeit von Finanzunternehmen von den Dienstleistungen des betreffenden IKT-Drittdienstleisters mit Blick auf kritische oder wichtige Funktionen von Finanzunternehmen, in die letztlich derselbe IKT-Drittdienstleister involviert ist — unabhängig davon, ob Finanzunternehmen diese Dienste direkt oder indirekt durch Vereinbarungen über die Unterauftragsvergabe in Anspruch nehmen;

d) dem Grad der Substituierbarkeit des IKT-Drittdienstleisters unter Berücksichtigung der folgenden Parameter:

   i) des Mangels an echten, auch teilweisen Alternativen aufgrund der begrenzten Zahl von IKT-Drittdienstleistern, die auf einem bestimmten Markt tätig sind, oder des Marktanteils des betreffenden IKT-Drittdienstleisters oder der damit verbundenen technischen Komplexität oder Differenziertheit, auch in Bezug auf proprietäre Technologien, oder der besonderen Merkmale der Organisation oder Tätigkeit des IKT-Drittdienstleisters;

   ii) der Schwierigkeiten bei der teilweisen oder vollständigen Migration der einschlägigen Daten und Arbeitslasten vom jeweiligen IKT-Drittdienstleister zu einem anderen IKT-Drittdienstleister, die entweder auf erhebliche finanzielle Kosten, zeitliche oder sonstige Ressourcen, die der Migrationsprozess mit sich bringen kann, oder auf erhöhte IKT-Risiken oder sonstige operationelle Risiken zurückzuführen sind, denen das Finanzunternehmen durch eine solche Migration ausgesetzt sein könnte.

(3) Gehört der IKT-Drittdienstleister zu einer Gruppe, so werden die in Absatz 2 genannten Kriterien in Bezug auf die von der Gruppe als Ganzes bereitgestellten IKT-Dienstleistungen berücksichtigt.

(4) Kritische IKT-Drittdienstleister, die Teil einer Gruppe sind, benennen eine juristische Person als Koordinierungsstelle, um eine angemessene Vertretung und Kommunikation mit der federführenden Überwachungsbehörde sicherzustellen.

(5) Die federführende Überwachungsbehörde unterrichtet den IKT-Drittdienstleister über das Ergebnis der Bewertung, die zu der in Absatz 1 Buchstabe a genannten Einstufung geführt hat. Innerhalb von sechs Wochen ab dem Datum der Unterrichtung kann der IKT-Drittdienstleister der federführenden Überwachungsbehörde eine begründete Erklärung mit allen für die Zwecke der Bewertung relevanten Informationen übermitteln. Die federführende Überwachungsbehörde prüft die begründete Erklärung und kann verlangen, dass innerhalb von 30 Kalendertagen nach Eingang der Erklärung zusätzliche Informationen übermittelt werden.

Nach der Einstufung eines IKT-Drittdienstleisters als kritisch, unterrichten die ESA den IKT-Drittdienstleister über den Gemeinsamen Ausschuss über diese Einstufung und das Anfangsdatum, ab dem er tatsächlich Überwachungstätigkeiten unterliegen wird. Dieses Anfangsdatum darf nicht mehr als einen Monat nach der Unterrichtung liegen. Der IKT-Drittdienstleister teilt den Finanzunternehmen, für die er Dienstleistungen erbringt, seine Einstufung als kritisch mit.

(6) Der Kommission wird die Befugnis übertragen, gemäß Artikel 57 einen delegierten Rechtsakt zu erlassen, um diese Verordnung durch die weitere Präzisierung der in Absatz 2 genannten Kriterien bis 17. Juli 2024 zu ergänzen.

(7) Die Einstufung nach Absatz 1 Buchstabe a darf erst angewendet werden, wenn die Kommission einen delegierten Rechtsakt gemäß Absatz 6 erlassen hat.

(8) Die Einstufung nach Absatz 1 Buchstabe a gilt nicht für:

i) Finanzunternehmen, die IKT-Dienstleistungen für andere Finanzunternehmen bereitstellen;

ii) IKT-Drittdienstleister, die Überwachungsrahmen unterliegen, die zur Unterstützung der in Artikel 127 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union genannten Aufgaben eingerichtet wurden;

iii) gruppeninterne IKT-Dienstleister;

iv) IKT-Drittdienstleister, die IKT-Dienstleistungen ausschließlich in einem Mitgliedstaat für Finanzunternehmen bereitstellen, die nur in diesem Mitgliedstaat tätig sind.

(9) Die ESA erstellen, veröffentlichen und aktualisieren die Liste kritischer IKT-Drittdienstleister auf Unionsebene jährlich über den Gemeinsamen Ausschuss.

(10) Die zuständigen Behörden übermitteln dem gemäß Artikel 32 eingerichteten Überwachungsforum für die Zwecke von Absatz 1 Buchstabe a die in Artikel 28 Absatz 3 Unterabsatz 3 genannten Berichte auf jährlicher und aggregierter Basis. Das Überwachungsforum bewertet die Abhängigkeiten von Finanzunternehmen gegenüber IKT-Drittdienstleistern auf der Grundlage der von den zuständigen Behörden übermittelten Informationen.

(11) Diejenigen IKT-Drittdienstleister, die nicht in der in Absatz 9 genannten Liste aufgeführt sind, können beantragen, gemäß Absatz 1 Buchstabe a als kritisch eingestuft zu werden.

Für die Zwecke von Unterabsatz 1 reicht der IKT-Drittdienstleister bei der EBA, der ESMA oder der EIOPA einen begründeten Antrag ein, die über den Gemeinsamen Ausschuss entscheiden, ob dieser IKT-Drittdienstleister gemäß Absatz 1 Buchstabe a als kritisch eingestuft werden soll.

Die in Unterabsatz 2 genannte Entscheidung wird innerhalb von 6 Monaten nach Eingang des Antrags getroffen und dem IKT-Drittdienstleister mitgeteilt.

(12) Finanzunternehmen dürfen nur dann die Dienstleistungen eines IKT-Drittdienstleisters mit Sitz in einem Drittland in Anspruch nehmen, der gemäß Absatz 1 Buchstabe a als kritisch eingestuft worden ist, wenn er innerhalb von zwölf Monaten nach der Einstufung ein Tochterunternehmen in der Union gegründet hat.

(13) Der in Absatz 12 genannte kritische IKT-Drittdienstleister teilt der federführenden Überwachungsbehörde jede Änderung der Leitungsstruktur des in der Union niedergelassenen Tochterunternehmens mit.

Artikel 32

Struktur des Überwachungsrahmens

(1) Der Gemeinsame Ausschuss richtet gemäß Artikel 57 Absatz 1 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 das Überwachungsforum als Unterausschuss ein, der die Arbeit des Gemeinsamen Ausschusses und der in Artikel 31 Absatz 1 Buchstabe b genannten federführenden Überwachungsbehörde im Bereich des IKT-Drittparteienrisikos in allen Finanzsektoren unterstützt. Das Überwachungsforum erarbeitet die Entwürfe gemeinsamer Positionen und gemeinsamer Maßnahmen des Gemeinsamen Ausschusses in diesem Bereich.

Das Überwachungsforum erörtert regelmäßig einschlägige Entwicklungen in Bezug auf IKT-Risiken und -Schwachstellen und fördert einen kohärenten Ansatz bei der Überwachung des IKT-Drittparteienrisikos auf Unionsebene.

(2) Das Überwachungsforum führt jährlich eine gemeinsame Bewertung der Ergebnisse und Erkenntnisse der Überwachungstätigkeiten durch, die für alle kritischen IKT-Drittdienstleister durchgeführt wurden, und fördert Koordinierungsmaßnahmen, um die digitale operationale Resilienz von Finanzunternehmen zu erhöhen, bewährte Verfahren zum Angehen des IKT-Konzentrationsrisikos zu fördern und Möglichkeiten zur Abschwächung sektorübergreifender Risikotransfers zu untersuchen.

(3) Das Überwachungsforum legt umfassende Referenzwerte für kritische IKT-Drittdienstleister vor, die vom Gemeinsamen Ausschuss als gemeinsame Positionen der ESA gemäß Artikel 56 Absatz 1 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 anzunehmen sind.

(4) Das Überwachungsforum setzt sich zusammen aus

a) den Vorsitzenden der ESA;

b) einem hochrangigen Vertreter des aktuellen Personals der in Artikel 46 genannten betreffenden zuständigen Behörde eines jeden Mitgliedstaats;

c) den Exekutivdirektoren jeder Europäischen Aufsichtsbehörde und einem Vertreter der Kommission, des ESRB, der EZB und der ENISA als Beobachter;

d) gegebenenfalls einem zusätzlichen Vertreter einer in Artikel 46 genannten zuständigen Behörde eines jeden Mitgliedstaats als Beobachter;

e) gegebenenfalls einem Vertreter der gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden, der für die Beaufsichtigung eines wesentlichen oder wichtigen, von der genannten Richtlinie erfassten Unternehmens, das als kritischer IKT-Drittdienstleister eingestuft wurde, zuständig ist, als Beobachter.

Das Überwachungsforum kann gegebenenfalls den Rat unabhängiger Sachverständiger einholen, die gemäß Absatz 6 ernannt wurden.

(5) Jeder Mitgliedstaat benennt die jeweils zuständige Behörde, deren Mitarbeiter der in Absatz 4 Unterabsatz 1 Buchstabe b genannte hochrangige Vertreter ist, und setzt die federführende Überwachungsbehörde davon in Kenntnis.

Die ESA veröffentlichen auf ihrer Website die Liste der von den Mitgliedstaaten benannten hochrangigen Vertreter aus dem aktuellen Personal der jeweils zuständigen Behörde.

(6) Die in Absatz 4 Unterabsatz 2 genannten unabhängigen Sachverständigen werden vom Überwachungsforum aus einem Pool von Sachverständigen ernannt, die im Anschluss an ein öffentliches und transparentes Bewerbungsverfahren ausgewählt wurden.

Die unabhängigen Sachverständigen werden auf der Grundlage ihres Fachwissens in den Bereichen Finanzstabilität, digitale operationale Resilienz und Fragen der IKT-Sicherheit ernannt. Sie handeln unabhängig und objektiv im alleinigen Interesse der Union als Ganzes und dürfen von Organen oder Einrichtungen der Union, von der Regierung eines Mitgliedstaats oder von öffentlichen oder privaten Stellen Weisungen weder einholen noch entgegennehmen.

(7) Gemäß Artikel 16 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 geben die ESA für die Zwecke dieses Abschnitts bis zum 17. Juli 2024 Leitlinien für die Zusammenarbeit zwischen den ESA und den zuständigen Behörden heraus, die die detaillierten Verfahren und Bedingungen für die Zuweisung und Ausführung von Aufgaben zwischen zuständigen Behörden und den ESA sowie die Einzelheiten zum Austausch von Informationen regeln, die zuständige Behörden benötigen, um die Weiterbehandlung der in Artikel 35 Absatz 1 Buchstabe d genannten Empfehlungen zu gewährleisten, die an kritische IKT-Drittdienstleister gerichtet werden.

(8) Die in diesem Abschnitt dargelegten Anforderungen gelten unbeschadet der Anwendung der Richtlinie (EU) 2022/2555 und anderer Überwachungsvorschriften der Union, die für Anbieter von Cloud-Computing-Diensten gelten.

(9) Die ESA legen dem Europäischen Parlament, dem Rat und der Kommission über den Gemeinsamen Ausschuss und auf der Grundlage von Vorarbeiten des Überwachungsforums jährlich einen Bericht über die Anwendung dieses Abschnitts vor.

Artikel 33

Aufgaben der federführenden Überwachungsbehörde

(1) Die gemäß Artikel 31 Absatz 1 Buchstabe b ernannte federführende Überwachungsbehörde führt die Überwachung über die zugewiesenen kritischen IKT-Drittdienstleister durch und ist für diese kritischen IKT-Drittdienstleister für die Zwecke aller mit der Überwachung verbundenen Angelegenheiten die vorrangige Anlaufstelle.

(2) Für die Zwecke des Absatzes 1 bewertet die federführende Überwachungsbehörde, ob jeder kritische IKT-Drittdienstleister über umfassende, fundierte und wirksame Vorschriften, Verfahren, Mechanismen und Vorkehrungen für das Management der IKT-Risiken verfügt, die er für Finanzunternehmen mit sich bringen kann.

Bei der in Unterabsatz 1 genannten Bewertung stehen vor allem IKT-Dienstleistungen im Mittelpunkt, die von dem kritischen IKT-Drittdienstleister bereitgestellt werden und kritische oder wichtige Funktionen von Finanzunternehmen unterstützen. Diese Bewertung wird auf IKT-Dienstleistungen, die andere als kritische oder wichtige Funktionen unterstützen, ausgeweitet, wenn dies zur Bewältigung aller relevanten Risiken erforderlich ist.

(3) Die in Absatz 2 genannte Bewertung erstreckt sich auf

a) IKT-Anforderungen, um insbesondere die Sicherheit, Verfügbarkeit, Kontinuität, Skalierbarkeit und Qualität der Dienste zu gewährleisten, die der kritische IKT-Drittdienstleister für Finanzunternehmen erbringt, sowie die Fähigkeit, jederzeit hohe Standards in Bezug auf Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der Daten aufrechtzuerhalten;

b) die physische Sicherheit, die zur Gewährleistung der IKT-Sicherheit beiträgt, darunter auch die Sicherheit von Räumlichkeiten, Einrichtungen und Datenzentren;

c) Risikomanagementprozesse, einschließlich Strategien für IKT-Risikomanagement, IKT-Geschäftsfortführungsleitlinie und IKT-Reaktions- und Wiederherstellungsplänen;

d) Governance-Regelungen, einschließlich einer Organisationsstruktur mit klaren, transparenten und kohärenten Zuständigkeits- und Rechenschaftspflichten, die ein wirksames IKT-Risikomanagement ermöglichen;

e) die Ermittlung, Überwachung und unverzügliche Meldung wesentlicher IKT-bezogener Vorfälle an die Finanzunternehmen sowie den Umgang mit und die Lösung dieser Vorfälle, insbesondere Cyberangriffe;

f) Mechanismen für Datenübertragbarkeit, Übertragbarkeit von Anwendungen und Interoperabilität, die eine wirksame Wahrnehmung von Kündigungsrechten durch die Finanzunternehmen gewährleisten;

g) Tests von IKT-Systemen, Infrastrukturen und Kontrollen;

h) IKT-Audits;

i) die Übernahme einschlägiger nationaler und internationaler Normen, die auf die Erbringung der IKT-Dienstleistungen für Finanzunternehmen anwendbar sind.

(4) Die federführende Überwachungsbehörde nimmt auf der Grundlage der in Absatz 2 genannten Bewertung und in Abstimmung mit dem in Artikel 34 Absatz 1 genannten gemeinsamen Überwachungsnetz (Joint Oversight Network — JON) einen klaren, detaillierten und durchdachten individuellen Überwachungsplan an, in dem die für jeden kritischen IKT-Drittdienstleister vorgesehenen jährlichen Überwachungsziele und wichtigsten Überwachungsmaßnahmen beschrieben werden. Dieser Plan wird dem kritischen IKT-Drittdienstleister jedes Jahr übermittelt.

Vor der Annahme des Überwachungsplans übermittelt die federführende Überwachungsbehörde dem kritischen IKT-Drittdienstleister den Entwurf des Überwachungsplans.

Nach Eingang des Entwurfs des Überwachungsplans kann der kritische IKT-Drittdienstleister innerhalb von 15 Kalendertagen eine begründete Erklärung vorlegen, in der die erwarteten Auswirkungen auf Kunden, bei denen es sich um nicht in den Anwendungsbereich dieser Verordnung fallende Unternehmen handelt, aufgezeigt werden und gegebenenfalls Lösungen zur Risikominderung enthalten sind.

(5) Sobald die in Absatz 4 genannten jährlichen Überwachungspläne angenommen und den kritischen IKT-Drittdienstleistern übermittelt wurden, dürfen die zuständigen Behörden Maßnahmen in Bezug auf diese kritischen IKT-Drittdienstleister nur im Einvernehmen mit der federführenden Überwachungsbehörde ergreifen.

Artikel 34

Operative Zusammenarbeit zwischen den federführenden Überwachungsbehörden

(1) Um einen kohärenten Ansatz bei den Überwachungstätigkeiten sicherzustellen und um koordinierte allgemeine Überwachungsstrategien und kohärente operative Ansätze und Arbeitsmethoden sicherzustellen, richten die drei gemäß Artikel 31 Absatz 1 Buchstabe b benannten federführenden Überwachungsbehörden ein JON ein, um sich in den Vorbereitungsphasen untereinander abzustimmen und die Überwachung über die von ihnen jeweils überwachten kritischen IKT-Drittdienstleister sowie über das etwaige Vorgehen, das gemäß Artikel 42 erforderlich sein könnte, zu koordinieren.

(2) Für die Zwecke von Absatz 1 erstellen die federführenden Überwachungsbehörden ein gemeinsames Überwachungsprotokoll, in dem die genauen Verfahren für die tägliche Koordinierung und die Gewährleistung eines raschen Austauschs und rascher Reaktionen festgelegt sind. Das Protokoll wird regelmäßig überarbeitet, um den operativen Erfordernissen, insbesondere der Entwicklung praktischer Überwachungsregelungen, Rechnung zu tragen.

(3) Die federführenden Überwachungsbehörden können die EZB und die ENISA auf Ad-hoc-Basis ersuchen, fachliche Beratung zu leisten, praktische Erfahrungen auszutauschen oder an spezifischen Koordinierungssitzungen des JON teilzunehmen.

Artikel 35

Befugnisse der federführenden Überwachungsbehörde

(1) Die federführende Überwachungsbehörde hat zur Wahrnehmung der in diesem Abschnitt dargelegten Aufgaben in Bezug auf die kritischen IKT-Drittdienstleister die Befugnis,

a) alle einschlägigen Informationen und Unterlagen gemäß Artikel 37 anzufordern;

b) allgemeine Untersuchungen und Inspektionen gemäß den Artikeln 38 bzw. 39 durchzuführen;

c) nach Abschluss der Überwachungstätigkeiten Berichte anzufordern, in denen die ergriffenen Maßnahmen oder die Abhilfemaßnahmen aufgeführt sind, die von den kritischen IKT-Drittdienstleistern in Bezug auf die in Buchstabe d dieses Absatzes genannten Empfehlungen ergriffen wurden;

d) Empfehlungen zu den in Artikel 33 Absatz 3 genannten Bereichen abzugeben, insbesondere in Bezug auf Folgendes:

   i) die Anwendung spezifischer IKT-Sicherheits- und Qualitätsanforderungen oder -verfahren, insbesondere in Bezug auf die Herausgabe von Patches, Aktualisierungen, Verschlüsselung und andere Sicherheitsmaßnahmen, die die federführende Überwachungsbehörde für die Gewährleistung der IKT-Sicherheit von Diensten, die Finanzunternehmen bereitgestellt werden, für relevant hält;

   ii) die Verwendung von Bedingungen — einschließlich ihrer technischen Umsetzung — zu denen die kritischen IKT-Drittdienstleister IKT-Dienstleistungen für Finanzunternehmen bereitstellen, die die federführende Überwachungsbehörde für relevant hält, um die Entstehung punktueller Ausfälle oder deren Verstärkung zu verhindern oder um mögliche systemische Auswirkungen im Finanzsektor der Union im Falle eines IKT-Konzentrationsrisikos zu minimieren;

   iii) jede geplante Unterauftragsvergabe, in deren Fall die federführende Überwachungsbehörde aufgrund der Prüfung der gemäß den Artikeln 37 und 38 erlangten Informationen der Auffassung ist, dass eine weitere Unterauftragsvergabe, einschließlich Vereinbarungen über die Unterauftragsvergabe, die die kritischen IKT-Drittdienstleister mit anderen IKT-Drittdienstleistern oder mit IKT-Unterauftragnehmern mit Sitz in einem Drittland zu schließen beabsichtigen, Risiken für die Erbringung von Dienstleistungen durch das Finanzunternehmen oder Risiken für die Finanzstabilität mit sich bringen kann;

   iv) von der Vereinbarung über weitere Unterauftragsvergabe abzusehen, wenn die folgenden kumulativen Bedingungen erfüllt sind:

      — Bei dem ausgewählten Unterauftragnehmer handelt es sich um einen IKT-Drittdienstleister oder einen IKT-Unterauftragnehmer mit Sitz in einem Drittland;

      — die Unterauftragsvergabe betrifft eine kritische oder wichtige Funktion des Finanzunternehmens; und

— die federführende Überwachungsbehörde ist der Ansicht, dass diese Unterauftragsvergabe ein eindeutiges und ernstes Risiko für die Finanzstabilität der Union oder für Finanzunternehmen darstellt, einschließlich der Fähigkeit von Finanzunternehmen, Aufsichtsanforderungen zu erfüllen.

Für die Zwecke der Ziffer iv des vorliegenden Buchstabens übermitteln IKT-Drittdienstleister der federführenden Überwachungsbehörde unter Verwendung der in Artikel 41 Absatz 1 Buchstabe b genannten Vorlage Informationen über die Unterauftragsvergabe.

(2) Bei der Ausübung der in diesem Artikel genannten Befugnisse geht die federführende Überwachungsbehörde wie folgt vor:

a) Sie sorgt für eine regelmäßige Abstimmung innerhalb des JON und bemüht sich gegebenenfalls insbesondere um kohärente Herangehensweisen für die Überwachung kritischer IKT-Drittdienstleister;

b) sie trägt dem durch die Richtlinie (EU) 2022/2555 geschaffenen Rahmen gebührend Rechnung und konsultiert erforderlichenfalls die gemäß der genannten Richtlinie benannten oder eingerichteten zuständigen Behörden, um eine Überschneidung von technischen und organisatorischen Maßnahmen zu vermeiden, die gemäß der genannten Richtlinie auf kritische IKT-Drittdienstleister angewandt werden könnten;

c) sie ist bestrebt, das Risiko einer Störung der Dienste, die von kritischen IKT-Drittdienstleistern für Kunden bereitgestellt werden, bei denen es sich um nicht in den Anwendungsbereich dieser Verordnung fallende Unternehmen handelt, so weit wie möglich zu minimieren.

(3) Die federführende Überwachungsbehörde konsultiert das Überwachungsforum, bevor sie die in Absatz 1 genannten Befugnisse ausübt.

Bevor die federführende Überwachungsbehörde Empfehlungen gemäß Absatz 1 Buchstabe d abgibt, bietet die sie dem IKT-Drittdienstleister Gelegenheit, innerhalb von 30 Kalendertagen einschlägige Informationen bereitzustellen, mit denen die erwarteten Auswirkungen auf Kunden, bei denen es sich um nicht in den Anwendungsbereich dieser Verordnung fallende Unternehmen handelt, aufgezeigt werden und die gegebenenfalls Lösungen zur Risikominderung enthalten.

(4) Die federführende Überwachungsbehörde unterrichtet das JON über das Ergebnis der Ausübung der in Absatz 1 Buchstaben a und b genannten Befugnisse. Sie übermittelt die in Absatz 1 Buchstabe c genannten Berichte unverzüglich dem JON und den Behörden, die für diejenigen Finanzunternehmen, die die IKT-Dienstleistungen des betreffenden kritischen IKT-Drittdienstleisters in Anspruch nehmen, zuständig sind.

(5) Kritische IKT-Drittdienstleister arbeiten nach Treu und Glauben mit der federführenden Überwachungsbehörde zusammen und unterstützen sie bei der Erfüllung ihrer Aufgaben.

(6) Bei vollständiger oder teilweiser Nichteinhaltung der Maßnahmen, die infolge der Ausübung der Befugnisse gemäß Absatz 1 Buchstaben a, b oder c zu ergreifen sind, und nach Ablauf einer Frist von mindestens 30 Kalendertagen ab dem Tag, an dem der kritische IKT-Drittdienstleister eine Mitteilung über die betreffenden Maßnahmen erhalten hat, erlässt die federführende Überwachungsbehörde eine Entscheidung über die Verhängung eines Zwangsgelds, um den kritischen IKT-Drittdienstleister zur Einhaltung dieser Maßnahmen zu zwingen.

(7) Das in Absatz 6 genannte Zwangsgeld wird täglich bis zur Einhaltung der Vorschriften und für höchstens sechs Monate nach Mitteilung der Entscheidung über die Verhängung eines Zwangsgelds an den kritischen IKT-Drittdienstleister verhängt.

(8) Die Höhe des Zwangsgelds, berechnet ab dem in der Entscheidung über die Verhängung des Zwangsgelds genannten Zeitpunkt, beträgt bis zu 1 % des durchschnittlichen weltweiten Tagesumsatzes, den der kritische IKT-Drittdienstleister im vorangegangenen Geschäftsjahr erzielt hat. Bei der Festsetzung der Höhe des Zwangsgelds berücksichtigt die federführende Überwachungsbehörde in Bezug auf die Nichteinhaltung der in Absatz 6 genannten Maßnahmen folgende Kriterien:

a) Schwere und Dauer der Nichteinhaltung;

b) ob die Nichteinhaltung vorsätzlich oder fahrlässig begangen wurde;

c) das Ausmaß der Zusammenarbeit des IKT-Drittdienstleisters mit der federführenden Überwachungsbehörde.

Für die Zwecke des Unterabsatzes 1 führt die federführende Überwachungsbehörde Konsultationen im Rahmen des JON durch, um einen konsistenten Ansatz sicherzustellen.

(9) Zwangsgelder sind administrativer Art und vollstreckbar. Die Zwangsvollstreckung erfolgt nach den geltenden Vorschriften des Zivilprozessrechts des Mitgliedstaats, in dessen Hoheitsgebiet Inspektionen und Zugang erfolgen. Die Gerichte des betreffenden Mitgliedstaats sind für Beschwerden im Zusammenhang mit vorschriftswidrigem Vollzug zuständig. Die Beträge der Zwangsgelder werden dem Gesamthaushaltsplan der Europäischen Union zugewiesen.

(10) Die federführende Überwachungsbehörde veröffentlicht sämtliche verhängten Zwangsgelder, sofern dies die Stabilität der Finanzmärkte nicht ernsthaft gefährdet und den Beteiligten daraus kein unverhältnismäßiger Schaden erwächst.

(11) Die federführende Überwachungsbehörde gibt den Vertretern des dem Verfahren unterliegenden kritischen IKT-Drittdienstleisters vor Verhängung eines Zwangsgeldes nach Absatz 6 Gelegenheit, zu den Feststellungen angehört zu werden, und stützt ihre Entscheidungen ausschließlich auf Feststellungen, zu denen sich der vom Verfahren betroffene kritische IKT-Drittdienstleister äußern konnte.

Die Verteidigungsrechte der vom Verfahren betroffenen Personen werden während des Verfahrens in vollem Umfang gewahrt. Der dem Verfahren unterworfene IKT-Drittdienstleister hat, vorbehaltlich des berechtigten Interesses anderer Personen an der Wahrung ihrer Geschäftsgeheimnisse, ein Recht auf Akteneinsicht. Vom Recht auf Akteneinsicht ausgenommen sind vertrauliche Informationen sowie interne vorbereitende Unterlagen der federführenden Überwachungsbehörde.

Artikel 36

Ausübung der Befugnisse der federführenden Überwachungsbehörde außerhalb der Union

(1) Wenn sich die Überwachungsziele im Wege der Interaktion mit dem für die Zwecke des Artikels 31 Absatz 12 gegründeten Tochterunternehmen oder durch Überwachungstätigkeiten an Standorten in der Union nicht erreichen lassen, kann die federführende Überwachungsbehörde an allen Standorten in einem Drittland, die sich im Eigentum eines kritischen IKT-Drittdienstleisters befinden oder von ihm zur Erbringung von Dienstleistungen für Finanzunternehmen der Union in irgendeiner Weise im Zusammenhang mit seiner Geschäftstätigkeit, seinen Funktionen oder seinen Dienstleistungen genutzt werden, wozu alle Verwaltungs-, Geschäfts- oder Betriebsstellen, Räumlichkeiten, Grundstücke, Gebäude oder andere Immobilien gehören, die Befugnisse ausüben, die in folgenden Bestimmungen genannt werden:

a) in Artikel 35 Absatz 1 Buchstabe a und

b) in Artikel 35 Absatz 1 Buchstabe b im Einklang mit Artikel 38 Absatz 2 Buchstaben a, b und d sowie in Artikel 39 Absatz 1 und Absatz 2 Buchstabe a.

Die in Unterabsatz 1 genannten Befugnisse können unter den folgenden Bedingungen ausgeübt werden:

i) Die federführende Überwachungsbehörde erachtet die Durchführung einer Inspektion in einem Drittland als notwendig, damit sie ihre Aufgaben entsprechend dieser Verordnung vollständig und wirksam wahrnehmen kann;

ii) die Inspektion in einem Drittland steht in direktem Zusammenhang mit der Bereitstellung von IKT-Dienstleistungen für Finanzunternehmen in der Union;

iii) der betreffende kritische IKT-Drittdienstleister stimmt der Durchführung einer Inspektion in einem Drittland zu; und

iv) die einschlägige Behörde des betreffenden Drittlands wurde von der federführenden Überwachungsbehörde offiziell unterrichtet und hat keine Einwände dagegen erhoben.

(2) Unbeschadet der jeweiligen Zuständigkeiten der Organe der Union und der Mitgliedstaaten schließen die EBA, die ESMA oder die EIOPA für die Zwecke des Absatzes 1 Vereinbarungen über die Verwaltungszusammenarbeit mit der einschlägigen Behörde des Drittlands, um die reibungslose Durchführung von Inspektionen in dem betreffenden Drittland durch die federführende Überwachungsbehörde und ihr für ihren Auftrag in diesem Drittland benanntes Team zu ermöglichen. Diese Kooperationsvereinbarungen begründen keine rechtlichen Verpflichtungen gegenüber der Union und ihren Mitgliedstaaten und hindern die Mitgliedstaaten und ihre zuständigen Behörden nicht daran, bilaterale oder multilaterale Vereinbarungen mit diesen Drittländern und deren einschlägigen Behörden zu schließen.

In den Kooperationsvereinbarungen sind mindestens die folgenden Elemente festgelegt:

a) die Verfahren für die Koordinierung der im Rahmen dieser Verordnung durchgeführten Überwachungstätigkeiten und jede entsprechende Überwachung des IKT-Drittparteienrisikos im Finanzsektor durch die einschlägige Behörde des betreffenden Drittlands, einschließlich der Einzelheiten für die Übermittlung der Zustimmung dieser Behörde, damit die federführende Überwachungsbehörde und ihr benanntes Team in dessen Hoheitsgebiet allgemeine Untersuchungen und Vor-Ort-Inspektionen gemäß Absatz 1 Unterabsatz 1 durchführen können;

b) der Mechanismus für die Übermittlung aller relevanten Informationen zwischen der EBA, der ESMA oder der EIOPA und der einschlägigen Behörde des betreffenden Drittlands, insbesondere im Zusammenhang mit Informationen, die von der federführenden Überwachungsbehörde gemäß Artikel 37 angefordert werden können;

c) die Mechanismen für die unverzügliche Unterrichtung der EBA, der ESMA oder der EIOPA durch die einschlägige Behörde des betreffenden Drittlands über Fälle, in denen einem IKT-Drittdienstleister mit Sitz in einem Drittland, der gemäß Artikel 31 Absatz 1 Buchstabe a als kritisch eingestuft wurde, ein Verstoß gegen die Anforderungen zur Last gelegt wird, die er nach dem geltenden Recht des betreffenden Drittlands bei der Erbringung von Dienstleistungen für Finanzinstitute in diesem Drittland einhalten muss, sowie die angewandten Rechtsbehelfe und verhängten Sanktionen;

d) die regelmäßige Übermittlung von Neuerungen im Bereich der regulatorischen und aufsichtlichen Entwicklungen bei der Überwachung des IKT-Drittparteienrisikos für Finanzinstitute in dem betreffenden Drittland;

e) die Einzelheiten, die erforderlichenfalls die Teilnahme eines Vertreters der zuständigen Drittlandsbehörde an den Inspektionen der federführenden Überwachungsbehörde und des benannten Teams ermöglichen.

(3) Ist die federführende Überwachungsbehörde nicht in der Lage, die in den Absätzen 1 und 2 genannten Überwachungstätigkeiten außerhalb der Union durchzuführen, so

a) übt sie ihre Befugnisse nach Artikel 35 auf der Grundlage aller ihr bekannten Tatsachen und zur Verfügung stehenden Unterlagen aus;

b) dokumentiert und erläutert sie alle Folgen, die sich daraus ergeben, dass sie nicht in der Lage ist, die geplanten Überwachungstätigkeiten gemäß diesem Artikel durchzuführen.

Die in Buchstabe b genannten potenziellen Folgen werden in den Empfehlungen der federführenden Überwachungsbehörde gemäß Artikel 35 Absatz 1 Buchstabe d berücksichtigt.

Artikel 37

Auskunftsersuchen

(1) Die federführende Überwachungsbehörde kann von kritischen IKT-Drittdienstleistern durch einfaches Ersuchen oder durch Beschluss verlangen, alle Informationen zur Verfügung zu stellen, die die federführende Überwachungsbehörde benötigt, um ihre Aufgaben im Rahmen dieser Verordnung wahrzunehmen, einschließlich aller relevanten Geschäfts- oder Betriebsunterlagen, Verträge, Leit- und Richtlinien, Dokumentationen, Meldungen über IKT-Sicherheitsprüfungen, Berichte über IKT-bezogene Vorfälle sowie aller Informationen über Parteien, an die der kritische IKT-Drittdienstleister betriebliche Funktionen oder Tätigkeiten ausgelagert hat.

(2) Bei der Übermittlung eines einfachen Auskunftsersuchens nach Absatz 1 verfährt die federführende Überwachungsbehörde wie folgt:

a) Sie nimmt auf diesen Artikel als Rechtsgrundlage des Ersuchens Bezug;

b) sie gibt den Zweck des Ersuchens bekannt;

c) sie erläutert, welche Informationen gefordert werden;

d) sie legt die Frist für die Vorlage der Informationen fest;

e) sie unterrichtet den Vertreter des kritischen IKT-Drittdienstleisters, von dem die Informationen angefordert werden, darüber, dass er zu deren Übermittlung zwar nicht verpflichtet ist, die vorgelegten Informationen bei freiwilliger Beantwortung des Ersuchens jedoch nicht falsch oder irreführend sein dürfen.

(3) Fordert die federführende Überwachungsbehörde durch entsprechenden Beschluss gemäß Absatz 1 Informationen an, verfährt sie wie folgt:

a) Sie nimmt auf diesen Artikel als Rechtsgrundlage des Ersuchens Bezug;

b) sie gibt den Zweck des Ersuchens bekannt;

c) sie erläutert, welche Informationen gefordert werden;

d) sie legt die Frist für die Vorlage der Informationen fest;

e) sie nennt die Zwangsgelder, die nach Artikel 35 Absatz 6 verhängt werden, wenn die geforderten Informationen unvollständig sind oder nicht innerhalb der unter Buchstabe d genannten Frist vorgelegt werden;

f) sie weist auf das Recht nach den Artikeln 60 und 61 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 hin, vor dem Beschwerdeausschuss der ESA Beschwerde gegen den Beschluss einzulegen und den Beschluss durch den Gerichtshof der Europäischen Union (im Folgenden „Gerichtshof") überprüfen zu lassen.

(4) Die Vertreter der kritischen IKT-Drittdienstleister stellen die angeforderten Informationen zur Verfügung. Ordnungsgemäß bevollmächtigte Rechtsanwälte können die Auskünfte im Namen ihrer Mandanten erteilen. Die kritischen IKT-Drittdienstleister bleiben in vollem Umfang verantwortlich, wenn die erteilten Auskünfte unvollständig, sachlich unrichtig oder irreführend sind.

(5) Die federführende Überwachungsbehörde übermittelt den für diejenigen Finanzunternehmen, die die Dienste der betreffenden kritischen IKT-Drittdienstleister nutzen, zuständigen Behörden sowie dem JON unverzüglich eine Kopie der Entscheidung, Informationen bereitzustellen.

Artikel 38

Allgemeine Untersuchungen

(1) Die federführende Überwachungsbehörde kann zur Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung mit Unterstützung des in Artikel 40 Absatz 1 genannten gemeinsamen Untersuchungsteams erforderlichenfalls Untersuchungen von kritischen IKT-Drittdienstleistern durchführen.

(2) Die federführende Überwachungsbehörde ist befugt,

a) Aufzeichnungen, Daten, Verfahren und sonstiges für die Erfüllung ihrer Aufgaben relevantes Material unabhängig von der Speicherform zu prüfen;

b) beglaubigte Kopien oder Auszüge dieser Aufzeichnungen, Daten und dokumentierten Verfahren und von sämtlichen sonstigen Materialien anzufertigen oder zu verlangen;

c) Vertreter des kritischen IKT-Drittdienstleisters vorzuladen und zur Abgabe mündlicher oder schriftlicher Erklärungen zu Sachverhalten oder Unterlagen aufzufordern, die mit Gegenstand und Zweck der Untersuchung in Zusammenhang stehen, und die Antworten aufzuzeichnen;

d) jede andere natürliche oder juristische Person zu befragen, die dieser Befragung zum Zweck der Einholung von Informationen über den Gegenstand einer Untersuchung zustimmt;

e) Aufzeichnungen von Telefongesprächen und Datenübermittlungen anzufordern.

(3) Die Bediensteten und sonstige von der federführenden Überwachungsbehörde zu Untersuchungen gemäß Absatz 1 ermächtigte Personen üben ihre Befugnisse unter Vorlage einer schriftlichen Ermächtigung aus, in der Gegenstand und Zweck der Untersuchung angegeben werden.

In der Ermächtigung sind auch die in Artikel 35 Absatz 6 vorgesehenen Zwangsgelder für den Fall anzugeben, dass die angeforderten Aufzeichnungen, Daten, dokumentierten Verfahren oder sonstigen Materialien oder die Antworten auf Fragen, die den Vertretern des IKT-Drittdienstleisters gestellt werden, nicht geliefert werden oder unvollständig sind.

(4) Die Vertreter der kritischen IKT-Drittdienstleister sind verpflichtet, sich den Untersuchungen auf der Grundlage einer Entscheidung der federführenden Überwachungsbehörde zu unterziehen. In dem Beschluss sind Gegenstand und Zweck der Untersuchung, die nach Artikel 35 Absatz 6 vorgesehenen Zwangsgelder, die nach den Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 möglichen Rechtsbehelfe sowie das Recht, den Beschluss durch den Gerichtshof überprüfen zu lassen, anzugeben.

(5) Rechtzeitig vor Beginn der Untersuchung unterrichtet die federführende Überwachungsbehörde die für diejenigen Finanzunternehmen, die die IKT-Dienstleistungen dieses kritischen IKT-Drittdienstleisters nutzen, zuständigen Behörden über die geplante Untersuchung sowie die Identität der bevollmächtigten Personen.

Die federführende Überwachungsbehörde übermittelt dem JON alle gemäß Unterabsatz 1 mitgeteilten Informationen.

Artikel 39

Inspektionen

(1) Die federführende Überwachungsbehörde kann zur Wahrnehmung ihrer Aufgaben nach dieser Verordnung mit Unterstützung der in Artikel 40 Absatz 1 genannten gemeinsamen Untersuchungsteams sämtliche Geschäftsräume, Grundstücke oder Gebäude des IKT-Drittdienstleisters, wie Hauptverwaltungen, Betriebszentren und sekundäre Räumlichkeiten, betreten und dort alle erforderlichen Vor-Ort-Inspektionen durchführen sowie außerhalb dieser Räumlichkeiten Inspektionen durchführen.

Für die Ausübung der in Unterabsatz 1 genannten Befugnisse konsultiert die federführende Überwachungsbehörde das JON.

(2) Die Bediensteten und sonstige Personen, die von der federführenden Überwachungsbehörde zur Durchführung einer Vor-Ort-Inspektion ermächtigt wurden, sind befugt,

a) diese Geschäftsräume, Grundstücke oder Gebäude zu betreten; und

b) diese Geschäftsräume, Bücher oder Aufzeichnungen für die Dauer der Inspektion und in dem für die Inspektion erforderlichen Umfang zu versiegeln.

Die Bediensteten und sonstige von der federführenden Überwachungsbehörde ermächtigten Personen üben ihre Befugnisse unter Vorlage einer schriftlichen Ermächtigung aus, in der Gegenstand und Zweck der Inspektion sowie die in Artikel 35 Absatz 6 vorgesehenen Zwangsgelder angegeben sind, die verhängt werden, wenn sich die Vertreter der betreffenden IKT-Drittdienstleister der Inspektion nicht unterziehen.

(3) Die federführende Überwachungsbehörde unterrichtet die für diejenigen Finanzunternehmen, die diesen IKT-Drittdienstleister in Anspruch nehmen, zuständigen Behörden rechtzeitig vor der Inspektion.

(4) Die Inspektionen erstrecken sich auf das gesamte Spektrum einschlägiger IKT-Systeme, -Netzwerke, -Geräte, -Informationen und -Daten, die für die Erbringung von IKT-Dienstleistungen für Finanzunternehmen verwendet werden oder dazu beitragen.

(5) Die federführende Überwachungsbehörde unterrichtet die kritischen IKT-Drittdienstleister vor jeder geplanten Vor-Ort-Inspektion mit angemessenem Vorlauf, es sei denn, eine solche Unterrichtung ist aufgrund einer Not- oder Krisensituation nicht möglich oder würde Umstände herbeiführen, unter denen die Inspektion oder das Audit nicht mehr wirksam wären.

(6) Der kritische IKT-Drittdienstleister unterzieht sich den durch Beschluss der federführenden Überwachungsbehörde angeordneten Vor-Ort-Inspektionen. In dem Beschluss sind Gegenstand, Zweck und Datum des Beginns der Inspektion, die nach Artikel 35 Absatz 6 vorgesehenen Zwangsgelder, die nach den Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 möglichen Rechtsbehelfe sowie das Recht, den Beschluss durch den Gerichtshof überprüfen zu lassen, anzugeben.

(7) Gelangen die Bediensteten und sonstige von der federführenden Überwachungsbehörde bevollmächtigte Personen zu dem Schluss, dass ein kritischer IKT-Drittdienstleister sich einer gemäß diesem Artikel angeordneten Inspektion widersetzt, unterrichtet die federführende Überwachungsbehörde den kritischen IKT-Drittdienstleister über die Folgen einer solchen Widersetzung, einschließlich der Möglichkeit der für die betreffenden Finanzunternehmen zuständigen Behörden, Finanzunternehmen zu verpflichten, die mit diesem kritischen IKT-Drittdienstleister geschlossenen vertraglichen Vereinbarungen zu kündigen.

Artikel 40

Laufende Überwachung

(1) Bei der Durchführung von Überwachungstätigkeiten, insbesondere allgemeinen Untersuchungen oder Inspektionen, wird die federführende Überwachungsbehörde von einem gemeinsamen Untersuchungsteam unterstützt, das für jeden kritischen IKT-Drittdienstleister eingerichtet wird.

(2) Das in Absatz 1 genannte gemeinsame Untersuchungsteam setzt sich aus Mitarbeitern der folgenden Behörden zusammen:

a) der ESA;

b) der jeweils zuständigen Behörden, die die Finanzunternehmen beaufsichtigen, denen der kritische IKT-Drittdienstleister IKT-Dienstleistungen erbringt;

c) der in Artikel 32 Absatz 4 Buchstabe e genannten zuständigen nationale Behörde, auf freiwilliger Basis;

d) einer zuständigen nationalen Behörde des Mitgliedstaats, in dem der kritische IKT-Drittdienstleister seinen Sitz hat, auf freiwilliger Basis.

Die Mitglieder des gemeinsamen Untersuchungsteams müssen über Fachwissen in den Bereichen IKT und operationelle Risiken verfügen. Das gemeinsame Untersuchungsteam arbeitet unter der Koordinierung eines benannten Mitarbeiters der federführenden Überwachungsbehörde („Koordinator der federführenden Überwachungsbehörde“).

(3) Innerhalb von 3 Monaten nach Abschluss einer Untersuchung oder Inspektion nimmt die federführende Überwachungsbehörde nach Konsultation des Überwachungsforums entsprechend den in Artikel 35 genannten Befugnissen an den kritischen IKT-Drittdienstleister zu richtende Empfehlungen an.

(4) Die in Absatz 3 genannten Empfehlungen werden dem kritischen IKT-Drittdienstleister und den für diejenigen Finanzunternehmen, denen er IKT-Dienstleistungen erbringt, zuständigen Behörden unverzüglich übermittelt.

Die federführende Überwachungsbehörde kann zur Erfüllung der Überwachungstätigkeiten alle einschlägigen Zertifizierungen Dritter und interne oder externe IKT-Prüfungsberichte Dritter berücksichtigen, die von dem kritischen IKT-Drittdienstleister zur Verfügung gestellt werden.

Artikel 41

Harmonisierung der Voraussetzungen für die Durchführung der Überwachungstätigkeiten

(1) Die ESA arbeiten über den Gemeinsamen Ausschuss Entwürfe technischer Regulierungsstandards aus, um Folgendes festzulegen:

a) die Informationen, die von einem IKT-Drittdienstleister in dem Antrag bereitzustellen sind, in dem gemäß Artikel 31 Absatz 11 freiwillig um Einstufung als kritisch ersucht wird;

b) Inhalt, Struktur und Format der Informationen, die IKT-Drittdienstleister gemäß Artikel 35 Absatz 1 übermitteln, offenlegen und melden müssen, einschließlich der Vorlage für die Bereitstellung von Informationen über die Vereinbarungen über die Unterauftragsvergabe;

c) die Kriterien für die Festlegung der Zusammensetzung des gemeinsamen Untersuchungsteams, bei der eine ausgewogene Beteiligung der Mitarbeiter der ESA und der jeweils zuständigen Behörden sicherzustellen ist, sowie ihrer Benennung, Aufgaben und Arbeitsvereinbarungen;

d) die Einzelheiten der von den zuständigen Behörden vorgenommenen Bewertung der Maßnahmen, die von kritischen IKT-Drittdienstleistern auf der Grundlage der Empfehlungen der federführenden Überwachungsbehörde gemäß Artikel 42 Absatz 3 ergriffen wurden.

(2) Die ESA legen der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Juli 2024 vor.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme technischer Regulierungsstandards nach Absatz 1 entsprechend dem Verfahren nach den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Artikel 42

Folgemaßnahmen zuständiger Behörden

(1) Kritische IKT-Drittdienstleister teilen entweder der federführenden Überwachungsbehörde innerhalb von 60 Kalendertagen nach Eingang der Empfehlungen, die von der federführenden Überwachungsbehörde gemäß Artikel 35 Absatz 1 Buchstabe d abgegeben werden, ihre Absicht mit, diesen Empfehlungen Folge zu leisten, oder legen eine begründete Erklärung für die Nichtbefolgung der Empfehlungen vor. Die federführende Überwachungsbehörde übermittelt diese Informationen unverzüglich den für das betreffende Finanzunternehmen zuständigen Behörden.

(2) Die federführende Überwachungsbehörde informiert öffentlich darüber, wenn ein kritischer IKT-Drittdienstleister es versäumt, die federführende Überwachungsbehörde gemäß Absatz 1 zu unterrichten, oder wenn die Erklärung des kritischen IKT-Drittdienstleisters als nicht ausreichend erachtet wird. Die veröffentlichten Informationen enthalten die Identität des kritischen IKT-Drittdienstleisters sowie Angaben über Art und Wesen der Nichtkonformität. Diese Informationen werden auf den zum Zweck der Gewährleistung der Sensibilisierung der Öffentlichkeit relevanten und angemessenen Umfang beschränkt, es sei denn eine solche Veröffentlichung würde den Beteiligten einen unverhältnismäßigen Schaden zufügen oder das ordnungsgemäße Funktionieren und die Integrität von Finanzmärkten oder die Stabilität des Finanzsystems der Union als Ganzes oder in Teilen gefährden.

Die federführende Überwachungsbehörde unterrichtet den IKT-Drittdienstleister über diese Veröffentlichung.

(3) Die zuständigen Behörden unterrichten die betreffenden Finanzunternehmen über die Risiken, die in den Empfehlungen an kritische IKT-Drittdienstleister gemäß Artikel 35 Absatz 1 Buchstabe d festgestellt wurden.

Beim Management des IKT-Drittparteienrisikos berücksichtigen die Finanzunternehmen die in Unterabsatz 1 genannten Risiken.

(4) Ist eine zuständige Behörde der Ansicht, dass ein Finanzunternehmen die in den Empfehlungen festgestellten spezifischen Risiken bei seinem Management der IKT-Drittparteienrisiken nicht oder nicht ausreichend berücksichtigt, teilt sie dem Finanzunternehmen mit, dass innerhalb von 60 Kalendertagen nach Eingang einer solchen Mitteilung eine Entscheidung gemäß Absatz 6 getroffen werden kann, falls keine geeigneten vertraglichen Vereinbarungen zur Beseitigung dieser Risiken bestehen.

(5) Nach Eingang der in Artikel 35 Absatz 1 Buchstabe c genannten Berichte und vor einer Entscheidung gemäß Absatz 6 können die zuständigen Behörden auf freiwilliger Basis die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden konsultieren, die für die Beaufsichtigung eines wesentlichen oder wichtigen, von der genannten Richtlinie erfassten Unternehmens, das als kritischer IKT-Drittdienstleister eingestuft wurde, zuständig sind.

(6) Im Einklang mit Artikel 50 können zuständige Behörden als letztes Mittel nach der Mitteilung und gegebenenfalls der Abstimmung gemäß den Absätzen 4 und 5 eine Entscheidung treffen, mit der sie von Finanzunternehmen verlangen, die Nutzung oder den Einsatz einer Dienstleistung, die von einem kritischen IKT-Drittdienstleister bereitgestellt wird, vorübergehend teilweise oder vollständig auszusetzen, bis die Risiken beseitigt sind, die in den an den kritischen IKT-Drittdienstleister gerichteten Empfehlungen festgestellt wurden. Die Behörden können von Finanzunternehmen erforderlichenfalls verlangen, die einschlägigen vertraglichen Vereinbarungen, die mit kritischen IKT-Drittdienstleistern geschlossen wurden, ganz oder teilweise zu kündigen.

(7) Verweigert ein kritischer IKT-Drittdienstleister die Befolgung der Empfehlungen, indem er einen anderen als den von der federführenden Überwachungsbehörde empfohlenen Ansatz wählt, und wirkt sich ein solcher abweichender Ansatz möglicherweise auf eine große Zahl von Finanzunternehmen oder einen erheblichen Teil des Finanzsektors negativ aus und haben einzelne Warnungen der zuständigen Behörden nicht zu kohärenten Ansätzen geführt, die das potenzielle Risiko für die Finanzstabilität mindern, kann die federführende Überwachungsbehörde nach Konsultation des Überwachungsforums den zuständigen Behörden gegebenenfalls unverbindliche und nicht für die Öffentlichkeit bestimmte Stellungnahmen übermitteln, um kohärente und konvergente aufsichtliche Folgemaßnahmen zu fördern.

(8) Nach Eingang der in Artikel 35 Absatz 1 Buchstabe c genannten Berichte berücksichtigen die zuständigen Behörden bei der in Absatz 6 genannten Entscheidung die Art und das Ausmaß des Risikos, das vom kritischen IKT-Drittdienstleister nicht angegangen wird, sowie die Schwere des Verstoßes unter Berücksichtigung der folgenden Kriterien:

a) der Schwere und Dauer des Verstoßes;

b) ob durch den Verstoß schwerwiegende Mängel in Bezug auf Verfahren, Managementsysteme, Risikomanagement und interne Kontrollen des kritischen IKT-Drittdienstleisters offengelegt wurden;

c) ob Wirtschaftskriminalität erleichtert oder herbeigeführt wurde oder auf andere Weise mit dem Verstoß in Verbindung steht;

d) ob der Verstoß vorsätzlich oder fahrlässig begangen wurde;

e) ob die Aussetzung oder Kündigung der vertraglichen Vereinbarungen ungeachtet der Bemühungen des Finanzunternehmens um Vermeidung von Störungen bei der Erbringung seiner Dienstleistungen ein Risiko für die Fortführung der Geschäftstätigkeit des Finanzunternehmens mit sich bringt;

f) gegebenenfalls der gemäß Absatz 5 auf freiwilliger Basis ersuchten Stellungnahme der gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden, die für die Beaufsichtigung eines wesentlichen oder wichtigen, von der genannten Richtlinie erfassten Unternehmens, das als kritischer IKT-Drittdienstleister eingestuft wurde, zuständig sind.

Die zuständigen Behörden gewähren Finanzunternehmen den erforderlichen Zeitraum, damit sie die vertraglichen Vereinbarungen mit kritischen IKT-Drittdienstleistern anpassen können, um nachteilige Auswirkungen auf ihre digitale operationale Resilienz zu vermeiden und ihnen die Anwendung der in Artikel 28 genannten Ausstiegsstrategien und Übergangspläne zu ermöglichen.

(9) Die Entscheidung gemäß Absatz 6 wird den in Artikel 32 Absatz 4 Buchstaben a, b und c genannten Mitgliedern des Überwachungsforums und dem JON mitgeteilt.

Die von den Entscheidungen gemäß Absatz 6 betroffenen kritischen IKT-Drittdienstleister arbeiten uneingeschränkt mit den betroffenen Finanzunternehmen zusammen, insbesondere im Zusammenhang mit dem Verfahren zur Aussetzung oder Kündigung ihrer vertraglichen Vereinbarungen.

(10) Die zuständigen Behörden unterrichten die federführende Überwachungsbehörde regelmäßig über die Herangehensweisen und Maßnahmen, die sie bei ihren Aufsichtsaufgaben in Bezug auf Finanzunternehmen gewählt haben, sowie über die von den Finanzunternehmen geschlossenen vertraglichen Vereinbarungen, wenn kritische IKT-Drittdienstleister Empfehlungen, die von der federführenden Überwachungsbehörde an sie gerichtet wurden, teilweise oder vollständig nicht befolgt haben.

(11) Die federführende Überwachungsbehörde kann auf Verlangen die zur Anleitung der zuständigen Behörden abgegebenen Empfehlungen näher erläutern.

Artikel 43

Überwachungsgebühren

(1) Die federführende Überwachungsbehörde erhebt gemäß dem in Absatz 2 genannten delegierten Rechtsakt von kritischen IKT-Drittdienstleistern Gebühren, die die notwendigen Ausgaben der federführenden Überwachungsbehörde für die Durchführung von Überwachungsaufgaben gemäß dieser Verordnung vollständig decken, einschließlich der Erstattung aller Kosten, die durch die Arbeit des in Artikel 40 genannten gemeinsamen Untersuchungsteams entstehen können, sowie der Kosten für die Beratung durch die in Artikel 32 Absatz 4 Unterabsatz 2 genannten unabhängigen Sachverständigen in Angelegenheiten, die in den Aufgabenbereich der direkten Überwachungstätigkeiten fallen.

Die Höhe einer Gebühr, die einem kritischen IKT-Drittdienstleister in Rechnung gestellt wird, deckt alle Kosten ab, die aufgrund der Erfüllung der in diesem Abschnitt festgelegten Aufgaben anfallen, und steht in einem angemessenen Verhältnis zu dessen Umsatz.

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 57 einen delegierten Rechtsakt zur Ergänzung dieser Verordnung durch Festlegung der Höhe der Gebühren und der Art und Weise ihrer Entrichtung bis zum 17. Juli 2024 zu erlassen.

Artikel 44

Internationale Zusammenarbeit

(1) Unbeschadet des Artikels 36 können die EBA, die ESMA und die EIOPA im Einklang mit Artikel 33 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1095/2010 bzw. (EU) Nr. 1094/2010 Verwaltungsvereinbarungen mit Regulierungs- und Überwachungsbehörden von Drittländern schließen, um die internationale Zusammenarbeit in Bezug auf das IKT-Drittparteienrisiko in verschiedenen Finanzsektoren zu fördern, insbesondere durch die Entwicklung bewährter Verfahren für die Überprüfung von IKT-Risikomanagementverfahren und -kontrollen, Abmilderungsmaßnahmen und Reaktionsmaßnahmen bei Vorfällen.

(2) Die ESA legen dem Europäischen Parlament, dem Rat und der Kommission über den Gemeinsamen Ausschuss alle fünf Jahre einen gemeinsamen vertraulichen Bericht vor, in dem die Ergebnisse einschlägiger Gespräche mit den in Absatz 1 genannten Behörden von Drittländern zusammengefasst werden, wobei der Schwerpunkt auf der Entwicklung des IKT-Drittparteienrisikos und den Auswirkungen auf die Finanzstabilität, die Marktintegrität, den Anlegerschutz und das Funktionieren des Binnenmarkts liegt.

KAPITEL VI

Vereinbarungen über den Austausch von Informationen

Artikel 45

Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen

(1) Finanzunternehmen können Informationen und Erkenntnisse über Cyberbedrohungen untereinander austauschen, einschließlich Indikatoren für Beeinträchtigungen, Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools, soweit dieser Austausch von Informationen und Erkenntnissen

a) darauf abzielt, die digitale operationale Resilienz von Finanzunternehmen zu stärken, insbesondere indem für Cyberbedrohungen sensibilisiert, die Verbreitung von Cyberbedrohungen eingeschränkt oder verhindert wird und die Verteidigungsfähigkeiten, Techniken zur Erkennung von Bedrohungen, Abmilderungsstrategien oder Phasen der Reaktion und Wiederherstellung unterstützt werden;

b) innerhalb vertrauenswürdiger Gemeinschaften von Finanzunternehmen erfolgt;

c) durch Vereinbarungen über den Austausch von Informationen umgesetzt wird, die den potenziell sensiblen Charakter der ausgetauschten Informationen schützen und Verhaltensregeln unterliegen, in deren Rahmen die Wahrung des Geschäftsgeheimnisses, der Schutz personenbezogener Daten im Einklang mit der Verordnung (EU) 2016/679 und Leitlinien für die Wettbewerbspolitik vollumfänglich befolgt werden.

(2) Für die Zwecke von Absatz 1 Buchstabe c werden in den Vereinbarungen über den Austausch von Informationen die Voraussetzungen für die Teilnahme und gegebenenfalls die Einzelheiten zur Einbindung staatlicher Behörden und der Eigenschaft, in der diese in die Vereinbarungen über den Austausch von Informationen eingebunden werden können, zur Einbindung von IKT-Drittdienstleistern sowie zu operativen Aspekten, einschließlich der Nutzung spezieller IT-Plattformen, festgelegt.

(3) Finanzunternehmen teilen zuständigen Behörden ihre Einbindung in die in Absatz 1 genannten Vereinbarungen über den Austausch von Informationen mit, sobald ihre Mitwirkung bestätigt wurde bzw. endet und diese Beendigung in Kraft ist.

KAPITEL VII

Zuständige Behörden

Artikel 46

Zuständige Behörden

Unbeschadet der Bestimmungen über den Überwachungsrahmen für kritische IKT-Drittdienstleister gemäß Kapitel V Abschnitt II dieser Verordnung wird die Einhaltung dieser Verordnung durch die folgenden zuständigen Behörden im Einklang mit den durch die jeweiligen Rechtsakte übertragenen Befugnissen sichergestellt:

a) bei Kreditinstituten sowie bei nach der Richtlinie 2013/36/EU ausgenommenen Instituten durch die gemäß Artikel 4 der genannten Richtlinie benannte zuständige Behörde und bei gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 als bedeutend eingestuften Kreditinstituten durch die EZB im Einklang mit den mittels der genannten Verordnung übertragenen Befugnissen und Aufgaben;

b) bei Zahlungsinstituten, einschließlich der nach der Richtlinie (EU) 2015/2366 ausgenommenen Zahlungsinstitute, bei E-Geld-Instituten, einschließlich der nach der Richtlinie 2009/110/EG ausgenommenen Institute, und bei den in Artikel 33 Absatz 1 der Richtlinie (EU) 2015/2366 genannten Kontoinformationsdienstleistern durch die gemäß Artikel 22 der Richtlinie (EU) 2015/2366 benannte zuständige Behörde;

c) bei Wertpapierfirmen durch die gemäß Artikel 4 der Richtlinie (EU) 2019/2034 des Europäischen Parlaments und des Rates ([38]) benannte zuständige Behörde;

d) bei gemäß der Verordnung über Märkte von Krypto-Werten zugelassenen Anbietern von Krypto-Dienstleistungen und Emittenten von an Vermögenswerte geknüpften Tokens durch die gemäß der entsprechenden Bestimmung der genannten Verordnung benannte zuständige Behörde;

e) bei Zentralverwahrern durch die gemäß Artikel 11 der Verordnung (EU) Nr. 909/2014 benannte zuständige Behörde;

f) bei zentralen Gegenparteien durch die gemäß Artikel 22 der Verordnung (EU) Nr. 648/2012 benannte zuständige Behörde;

g) bei Handelsplätzen und Datenbereitstellungsdiensten durch die gemäß Artikel 67 der Richtlinie 2014/65/EU benannte zuständige Behörde und die zuständige Behörde im Sinne von Artikel 2 Absatz 1 Nummer 18 der Verordnung (EU) Nr. 600/2014;

h) bei Transaktionsregistern durch die gemäß Artikel 22 der Verordnung (EU) Nr. 648/2012 benannte zuständige Behörde;

i) bei Verwaltern alternativer Investmentfonds durch die gemäß Artikel 44 der Richtlinie 2011/61/EU benannte zuständige Behörde;

j) bei Verwaltungsgesellschaften durch die gemäß Artikel 97 der Richtlinie 2009/65/EG benannte zuständige Behörde;

k) bei Versicherungs- und Rückversicherungsunternehmen durch die gemäß Artikel 30 der Richtlinie 2009/138/EG benannte zuständige Behörde;

l) bei Versicherungsvermittlern, Rückversicherungsvermittlern und Versicherungsvermittlern in Nebentätigkeit durch die gemäß Artikel 12 der Richtlinie (EU) 2016/97 benannte zuständige Behörde;

m) bei Einrichtungen der betrieblichen Altersversorgung durch die gemäß Artikel 47 der Richtlinie (EU) 2016/2341 benannte zuständige Behörde;

n) bei Ratingagenturen durch die gemäß Artikel 21 der Verordnung (EG) Nr. 1060/2009 benannte zuständige Behörde;

o) bei Administratoren kritischer Referenzwerte durch die gemäß den Artikeln 40 und 41 der Verordnung (EU) 2016/1011 benannte zuständige Behörde;

([38]) Richtlinie (EU) 2019/2034 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Beaufsichtigung von Wertpapierfirmen und zur Änderung der Richtlinien 2002/87/EG, 2009/65/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU und 2014/65/EU (ABl. L 314 vom 5.12.2019, S. 64).

p) bei Schwarmfinanzierungsdienstleistern durch die gemäß Artikel 29 der Verordnung (EU) 2020/1503 benannte zuständige Behörde;

q) bei Verbriefungsregistern durch die gemäß Artikel 10 und Artikel 14 Absatz 1 der Verordnung (EU) 2017/2402 benannte zuständige Behörde.

Artikel 47

Zusammenarbeit mit den durch die Richtlinie (EU) 2022/2555 geschaffenen Strukturen und Behörden

(1) Um die Zusammenarbeit zu fördern und den aufsichtlichen Austausch zwischen den gemäß dieser Verordnung benannten zuständigen Behörden und der durch Artikel 14 der Richtlinie (EU) 2022/2555 eingesetzten Kooperationsgruppe zu ermöglichen, können sich die ESA und die zuständigen Behörden bei Angelegenheiten, die ihre Aufsichtstätigkeiten in Bezug auf Finanzunternehmen betreffen, an den Tätigkeiten der Kooperationsgruppe beteiligen. Die ESA und die zuständigen Behörden können verlangen, zur Teilnahme an den Tätigkeiten der Kooperationsgruppe in Angelegenheiten im Zusammenhang mit den wesentlichen oder wichtigen, von der Richtlinie (EU) 2022/2555 erfassten Unternehmen, die ebenfalls gemäß Artikel 31 der vorliegenden Verordnung als kritische IKT-Drittdienstleister eingestuft wurden, eingeladen zu werden.

(2) Die zuständigen Behörden können sich gegebenenfalls an die zentralen Anlaufstellen und die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten CSIRT wenden und mit ihnen Informationen austauschen.

(3) Die zuständigen Behörden können gegebenenfalls die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden um einschlägige fachliche Beratung und Unterstützung ersuchen und Kooperationsvereinbarungen schließen, um die Einrichtung wirksamer und schneller Koordinierungsmechanismen zu ermöglichen.

(4) In den in Absatz 3 genannten Vereinbarungen können unter anderem Verfahren für die Koordinierung der Aufsichts- bzw. Überwachungstätigkeiten in Bezug auf wesentliche oder wichtige, von der Richtlinie (EU) 2022/2555 erfasste Unternehmen, die gemäß Artikel 31 der vorliegenden Verordnung als kritische IKT-Drittdienstleister eingestuft wurden, festgelegt werden, wozu die Durchführung von Untersuchungen und Vor-Ort-Inspektionen im Einklang mit dem nationalen Recht sowie Mechanismen für den Informationsaustausch zwischen den gemäß der vorliegenden Verordnung zuständigen Behörden und den gemäß der genannten Richtlinie benannten oder eingerichteten Behörden, einschließlich des Zugangs zu den von den letztgenannten Behörden angeforderten Informationen, gehören.

Artikel 48

Zusammenarbeit der Behörden

(1) Die zuständigen Behörden arbeiten untereinander und gegebenenfalls mit der federführenden Überwachungsbehörde eng zusammen.

(2) Die zuständigen Behörden und die federführende Überwachungsbehörde tauschen zeitnah alle relevanten Informationen über kritische IKT-Drittdienstleister aus, die sie benötigen, um ihre jeweiligen Aufgaben gemäß dieser Verordnung wahrnehmen zu können, insbesondere in Bezug auf die ermittelten Risiken, die Herangehensweisen und die Maßnahmen, die im Rahmen der Überwachungsaufgaben der federführenden Überwachungsbehörde ergriffen wurden.

Artikel 49

Sektorübergreifende Übungen, Kommunikation und Zusammenarbeit im Finanzbereich

(1) Die ESA können über den Gemeinsamen Ausschuss und in Zusammenarbeit mit — je nach Sachlage — den zuständigen Behörden, den in Artikel 3 der Richtlinie 2014/59/EU genannten nationalen Abwicklungsbehörden, der EZB, dem Einheitlichen Abwicklungsausschuss (bei Informationen über Unternehmen, die in den Geltungsbereich der Verordnung (EU) Nr. 806/2014 fallen), dem ESRB und der ENISA Mechanismen für den Austausch wirksamer Verfahren zwischen Finanzsektoren einrichten, um die Lageerfassung zu verbessern und sektorübergreifend gemeinsame Cyberanfälligkeiten und -risiken zu ermitteln.

Ebenso können sie Krisenmanagement- und Notfallübungen mit Szenarien für Cyberangriffe konzipieren, um Kommunikationskanäle zu entwickeln und schrittweise eine wirksame koordinierte Reaktion auf Unionsebene zu ermöglichen, sofern es zu einem schwerwiegenden grenzüberschreitenden IKT-bezogenen Vorfall oder einer vergleichbaren Bedrohung kommt, die systemische Auswirkungen auf den gesamten Finanzsektor der Union mit sich bringen.

Mit diesen Übungen können gegebenenfalls auch Abhängigkeiten des Finanzsektors von anderen Wirtschaftssektoren untersucht werden.

(2) Die zuständigen Behörden, die ESA und die EZB arbeiten eng zusammen und tauschen Informationen aus, um ihren Aufgaben gemäß den Artikeln 47 bis 54 nachzukommen. Dabei stimmen sie ihre Beaufsichtigungstätigkeit eng untereinander ab, um Verstöße gegen diese Verordnung festzustellen und ihnen entgegenzuwirken, bewährte Verfahren zu entwickeln und zu fördern, die Zusammenarbeit zu erleichtern, eine kohärente Auslegung zu fördern und bei Uneinigkeit eine Bewertung vorzunehmen, die sich nicht nur auf eine einzelne Rechtsordnung stützt.

Artikel 50

Verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen

(1) Die zuständigen Behörden verfügen über alle Aufsichts-, Untersuchungs- und Sanktionsbefugnisse, die zur Erfüllung ihrer Aufgaben im Rahmen dieser Verordnung erforderlich sind.

(2) Die Befugnisse gemäß Absatz 1 umfassen zumindest folgende Befugnisse:

a) den Zugriff auf Unterlagen oder Daten jeglicher Form, die nach Ansicht der zuständigen Behörde für die Ausführung ihrer Aufgaben von Belang sind, sowie den Erhalt oder Anfertigung von Kopien von ihnen;

b) Durchführung von Vor-Ort-Inspektionen oder Untersuchungen, einschließlich unter anderem

   i) der Vorladung von Vertretern der Finanzunternehmen, damit diese mündliche oder schriftliche Erklärungen zu Sachverhalten oder Unterlagen abgeben, die mit Gegenstand und Zweck der Untersuchung in Zusammenhang stehen, sowie der Aufzeichnung der Antworten,

   ii) der Befragung jeder anderen natürlichen oder juristischen Person, die dieser Befragung zum Zweck der Einholung von Informationen über den Gegenstand einer Untersuchung zustimmt;

c) das Verlangen von Korrektur- und Abhilfemaßnahmen bei Verstößen gegen die Anforderungen dieser Verordnung.

(3) Unbeschadet des Rechts der Mitgliedstaaten, strafrechtliche Sanktionen im Einklang mit Artikel 52 zu verhängen, legen die Mitgliedstaaten angemessene verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen für Verstöße gegen diese Verordnung fest und sorgen für deren wirksame Umsetzung.

Diese Sanktionen und Maßnahmen müssen wirksam, verhältnismäßig und abschreckend sein.

(4) Die Mitgliedstaaten übertragen den zuständigen Behörden die Befugnis, bei Verstößen gegen diese Verordnung mindestens die folgenden verwaltungsrechtlichen Sanktionen bzw. Abhilfemaßnahmen anzuwenden:

a) die Erteilung einer Anweisung, wonach die natürliche oder juristische Person gegen diese Verordnung verstoßendes Verhalten zu unterlassen und von einer Wiederholung abzusehen hat;

b) das Verlangen, dass Praktiken oder Verhaltensweisen, die nach Ansicht der zuständigen Behörde den Bestimmungen dieser Verordnung zuwiderlaufen, vorübergehend oder dauerhaft eingestellt und nicht wiederholt werden;

c) das Ergreifen jeder Art von Maßnahme, auch finanzieller Art, um sicherzustellen, dass Finanzunternehmen weiterhin die rechtlichen Anforderungen erfüllen;

d) das Verlangen — soweit gemäß nationalem Recht zulässig — bereits existierender Aufzeichnungen von Datenübermittlungen im Besitz einer Telekommunikationsgesellschaft, wenn der begründete Verdacht auf einen Verstoß gegen die Verordnung besteht und diese Aufzeichnungen für eine Untersuchung von Verstößen gegen diese Verordnung relevant sein könnten; und

e) die Abgabe öffentlicher Bekanntmachungen, einschließlich öffentlicher Bekanntgaben, in denen die Identität der natürlichen oder juristischen Person und die Art des Verstoßes angegeben sind.

(5) Gelten Absatz 2 Buchstabe c und Absatz 4 für juristische Personen, so statten die Mitgliedstaaten die zuständigen Behörden mit der Befugnis aus, Mitgliedern des Leitungsorgans sowie anderen natürlichen Personen, die nach nationalem Recht für den Verstoß verantwortlich sind, vorbehaltlich der nach nationalem Recht geltenden Bedingungen verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen aufzuerlegen.

(6) Die Mitgliedstaaten stellen sicher, dass alle Entscheidungen zur Auferlegung der in Absatz 2 Buchstabe c festgelegten verwaltungsrechtlichen Sanktionen oder Abhilfemaßnahmen ordnungsgemäß begründet werden und dass gegen sie ein Rechtsbehelf eingelegt werden kann.

Artikel 51

Ausübung der Befugnis zur Auferlegung von verwaltungsrechtlichen Sanktionen und Abhilfemaßnahmen

(1) Die zuständigen Behörden üben die Befugnisse zur Auferlegung der in Artikel 50 genannten verwaltungsrechtlichen Sanktionen und Abhilfemaßnahmen innerhalb ihres nationalen Rechtsrahmens je nach Sachlage in folgender Weise aus:

a) direkt;

b) in Zusammenarbeit mit anderen Behörden;

c) unter ihrer Verantwortung durch Übertragung an andere Behörden oder

d) durch Antragstellung bei den zuständigen Justizbehörden.

(2) Bei der Festlegung von Art und Umfang einer nach Artikel 50 auferlegten verwaltungsrechtlichen Sanktion oder Abhilfemaßnahme berücksichtigen die zuständigen Behörden, inwieweit der Verstoß vorsätzlich erfolgte oder das Ergebnis von Fahrlässigkeit ist, sowie alle anderen relevanten Umstände, darunter auch je nach Sachlage:

a) die Wesentlichkeit, Schwere und Dauer des Verstoßes;

b) der Grad an Verantwortung der für den Verstoß verantwortlichen natürlichen oder juristischen Person;

c) die Finanzkraft der verantwortlichen natürlichen oder juristischen Person;

d) die Höhe der von der verantwortlichen natürlichen oder juristischen Person erzielten Gewinne oder verhinderten Verluste, sofern sich diese beziffern lassen;

e) die Verluste, die Dritten durch den Verstoß entstanden sind, sofern sich diese beziffern lassen;

f) die Bereitschaft der verantwortlichen natürlichen oder juristischen Person zur Zusammenarbeit mit der zuständigen Behörde, unbeschadet des Erfordernisses, die von dieser natürlichen oder juristischen Person erzielten Gewinne oder verhinderten Verluste einzuziehen;

g) frühere Verstöße der verantwortlichen natürlichen oder juristischen Person.

Artikel 52

Strafrechtliche Sanktionen

(1) Mitgliedstaaten können beschließen, für Verstöße, die nach ihrem nationalen Recht strafrechtlichen Sanktionen unterliegen, keine Vorschriften für verwaltungsrechtliche Sanktionen oder Abhilfemaßnahmen festzulegen.

(2) Mitgliedstaaten, die strafrechtliche Sanktionen für die in dieser Verordnung genannten Verstöße festgelegt haben, stellen durch angemessene Maßnahmen sicher, dass die zuständigen Behörden über alle notwendigen Befugnisse verfügen, um sich mit den Justiz-, Strafverfolgungs- oder Strafjustizbehörden in ihrem Hoheitsgebiet ins Benehmen zu setzen, um spezifische Informationen im Zusammenhang mit strafrechtlichen Ermittlungen oder Verfahren, die wegen der Verstöße gegen diese Verordnung eingeleitet wurden, zu erhalten und diese anderen zuständigen Behörden sowie der EBA, der ESMA oder der EIOPA zur Verfügung zu stellen, um ihre Pflichten zur Zusammenarbeit für die Zwecke dieser Verordnung zu erfüllen.

Artikel 53

Mitteilungspflichten

Die Mitgliedstaaten teilen der Kommission, der ESMA, der EBA und der EIOPA bis zum 17. Januar 2025 die Gesetze, sonstige Vorschriften sowie Verwaltungsvorschriften, einschließlich der einschlägigen strafrechtlichen Vorschriften, zur Umsetzung dieses Kapitels mit. Die Mitgliedstaaten teilen der Kommission, der ESMA, der EBA und der EIOPA spätere Änderungen dieser Vorschriften unverzüglich mit.

Artikel 54

Öffentliche Bekanntmachung verwaltungsrechtlicher Sanktionen

(1) Die zuständigen Behörden veröffentlichen auf ihren amtlichen Websites unverzüglich jede Entscheidung zur Verhängung einer verwaltungsrechtlichen Sanktion, gegen die nach Mitteilung dieser Entscheidung an die Person, gegen die die Sanktion verhängt wurde, kein Rechtsbehelf eingelegt werden kann.

(2) Die in Absatz 1 genannte Bekanntmachung umfasst Informationen zu Art und Natur des Verstoßes, der Identität der verantwortlichen Personen und der verhängten Sanktionen.

(3) Gelangt die zuständige Behörde nach einer Einzelfallprüfung zu der Auffassung, dass die Bekanntmachung der Identität im Falle juristischer Personen oder der Identität und der personenbezogenen Daten im Falle natürlicher Personen unverhältnismäßig wäre, was auch Risiken für den Schutz personenbezogener Daten einschließt, die Stabilität der Finanzmärkte oder die Durchführung laufender strafrechtlicher Ermittlungen gefährden oder der betroffenen Person einen unverhältnismäßigen Schaden zufügen würde — soweit dieser ermittelt werden kann —, so beschließt sie in Bezug auf die Entscheidung, mit der eine verwaltungsrechtliche Sanktion verhängt wird, eine der folgenden Lösungen:

a) Aufschub der Veröffentlichung bis alle Gründe für die Nichtveröffentlichung wegfallen;

b) anonyme Veröffentlichung im Einklang mit dem nationalen Recht; oder

c) Unterlassung der Veröffentlichung, wenn die unter den Buchstaben a und b genannten Optionen entweder nicht ausreichen, um zu gewährleisten, dass keine Gefahr für die Stabilität der Finanzmärkte besteht, oder wenn eine solche Veröffentlichung nicht mit der bei der Verhängung der Sanktion angewandten Nachsicht vereinbar wäre.

(4) Wird entschieden, eine verwaltungsrechtliche Sanktion gemäß Absatz 3 Buchstabe b in anonymisierter Form bekannt zu machen, so kann die Bekanntmachung der einschlägigen Angaben aufgeschoben werden.

(5) Macht eine zuständige Behörde eine Entscheidung zur Verhängung einer verwaltungsrechtlichen Sanktion, gegen die ein Rechtsbehelf bei den einschlägigen Justizbehörden eingelegt worden ist, bekannt, so fügen die zuständigen Behörden diese Information ihrer amtlichen Website unverzüglich und etwaige nachfolgende Informationen über den Ausgang des Rechtsbehelfsverfahrens zu einem späteren Zeitpunkt hinzu. Gerichtliche Entscheidungen, mit denen eine Entscheidung zur Verhängung einer verwaltungsrechtlichen Sanktion für nichtig erklärt wird, werden ebenfalls bekannt gemacht.

(6) Die zuständigen Behörden stellen sicher, dass die in den Absätzen 1 bis 4 genannten Bekanntmachungen nur so lange auf ihrer amtlichen Website verbleiben, wie es zum Zwecke dieses Artikels erforderlich ist. Dieser Zeitraum darf fünf Jahre ab dem Zeitpunkt der Veröffentlichung nicht überschreiten.

Artikel 55

Wahrung des Berufsgeheimnisses

(1) Vertrauliche Informationen, die gemäß dieser Verordnung empfangen, ausgetauscht oder übermittelt werden, unterliegen den in Absatz 2 festgelegten Bestimmungen zum Berufsgeheimnis.

(2) Zur Wahrung des Berufsgeheimnisses verpflichtet sind alle Personen, die bei den gemäß dieser Verordnung zuständigen Behörden oder bei einer Behörde, einem Marktteilnehmer oder einer natürlichen oder juristischen Person beschäftigt sind oder waren, an die bzw. den diese zuständigen Behörden ihre Befugnisse delegiert haben, einschließlich unter Vertrag genommener Revisoren und Sachverständigen.

(3) Unter das Berufsgeheimnis fallende Informationen, einschließlich der zwischen den gemäß der vorliegenden Verordnung zuständigen Behörden und den gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden ausgetauschten Informationen, dürfen keiner anderen Person oder Behörde gegenüber offengelegt werden, es sei denn, dies geschieht aufgrund von Unionsrecht oder nationalem Recht.

(4) Alle gemäß dieser Verordnung zwischen den zuständigen Behörden ausgetauschten Informationen, die Geschäfts- oder Betriebsbedingungen und andere wirtschaftliche oder persönliche Angelegenheiten betreffen, werden als vertraulich betrachtet und unterliegen den Anforderungen an das Berufsgeheimnis, es sein denn, ihre Weitergabe wird von der zuständigen Behörde zum Zeitpunkt der Mitteilung für zulässig erklärt oder ist für Gerichtsverfahren erforderlich.

Artikel 56

Datenschutz

(1) Die ESA und die zuständigen Behörden dürfen personenbezogene Daten nur verarbeiten, wenn dies zur Erfüllung ihrer jeweiligen Pflichten und Aufgaben gemäß dieser Verordnung erforderlich ist, insbesondere für Untersuchungen, Inspektionen, Auskunftsersuchen, Kommunikationszwecke, Veröffentlichungen, Evaluierungen, Verifizierungen, Bewertungen und die Erstellung von Überwachungsplänen. Die personenbezogenen Daten müssen im Einklang mit der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 verarbeitet werden, je nachdem, welche der beiden anwendbar ist.

(2) Sofern in anderen sektorspezifischen Rechtsakten nichts anderes vorgesehen ist, werden die in Absatz 1 genannten personenbezogenen Daten bis zur Erfüllung der geltenden Aufsichtspflichten, in jedem Fall aber für höchstens 15 Jahre aufbewahrt, außer bei anhängigen Gerichtsverfahren, die eine weitere Speicherung dieser Daten erfordern.

KAPITEL VIII

Delegierte Rechtsakte

Artikel 57

Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 31 Absatz 6 und Artikel 43 Absatz 2 wird der Kommission für einen Zeitraum von fünf Jahren ab dem 17. Januar 2024 übertragen. Die Kommission erstellt spätestens neun Monate vor Ablauf des Zeitraums von fünf Jahren einen Bericht über die Befugnisübertragung. Die Befugnisübertragung verlängert sich stillschweigend um Zeiträume gleicher Länge, es sei denn, das Europäische Parlament oder der Rat widersprechen einer solchen Verlängerung spätestens drei Monate vor Ablauf des jeweiligen Zeitraums.

(3) Die Befugnisübertragung gemäß Artikel 31 Absatz 6 und Artikel 43 Absatz 2 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen, im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 31 Absatz 6 und Artikel 43 Absatz 2 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von drei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist sowohl das Europäische Parlament als auch der Rat der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um drei Monate verlängert.

KAPITEL IX

Übergangs- und Schlussbestimmungen

Abschnitt I

Artikel 58

Überprüfungsklausel

(1) Bis zum 17. Januar 2028 führt die Kommission nach Konsultation der ESA und des ESRB, je nach Sachlage, eine Überprüfung durch und legt dem Europäischen Parlament und dem Rat einen Bericht vor, gegebenenfalls zusammen mit einem Gesetzgebungsvorschlag. Die Überprüfung muss sich mindestens auf Folgendes erstrecken:

a) die Kriterien für die Benennung kritischer IKT-Drittdienstleister gemäß Artikel 31 Absatz 2;

b) die Freiwilligkeit der Meldung erheblicher Cyberbedrohungen gemäß Artikel 19;

c) die Regelung gemäß Artikel 31 Absatz 12 und die Befugnisse der federführenden Überwachungsbehörde gemäß Artikel 35 Absatz 1 Buchstabe d Ziffer iv erster Gedankenstrich, um die Wirksamkeit dieser Bestimmungen im Hinblick auf die Gewährleistung einer wirksamen Überwachung kritischer IKT-Drittdienstleister mit Sitz in einem Drittland und die Notwendigkeit der Gründung eines Tochterunternehmens in der Union zu bewerten.

   Für die Zwecke von Unterabsatz 1 dieses Buchstabens umfasst die Überprüfung eine Analyse der Regelung gemäß Artikel 31 Absatz 12, einschließlich hinsichtlich der Bedingungen für den Zugang von Finanzunternehmen der Union zu Dienstleistungen aus Drittländern und der Verfügbarkeit dieser Dienstleistungen auf dem Unionsmarkt, und berücksichtigt weitere Entwicklungen auf den Märkten für die unter diese Verordnung fallenden Dienstleistungen, die von Finanzunternehmen und Finanzaufsichtsbehörden bei der Anwendung dieser Regelung bzw. der damit verbundenen Beaufsichtigung gewonnenen praktischen Erfahrungen sowie alle einschlägigen regulatorischen und aufsichtlichen Entwicklungen auf internationaler Ebene.

d) die Angemessenheit der Einbeziehung derjenigen in Artikel 2 Absatz 3 Buchstabe e genannten Finanzunternehmen in den Geltungsbereich dieser Verordnung, die automatisierte Vertriebssysteme nutzen, unter Berücksichtigung künftiger Marktentwicklungen im Zusammenhang mit der Nutzung solcher Systeme;

e) die Funktionsweise und Wirksamkeit des JON bei der Förderung der Kohärenz der Überwachung und der Effizienz des Informationsaustauschs innerhalb des Überwachungsrahmens.

(2) Im Zusammenhang mit der Überprüfung der Richtlinie (EU) 2015/2366 bewertet die Kommission, ob die Resilienz von Zahlungssystemen und Zahlungsabwicklungstätigkeiten gegenüber Cyberangriffen erhöht werden muss und ob es angemessen ist, den Geltungsbereich dieser Verordnung auf Betreiber von Zahlungssystemen und an Zahlungsabwicklungstätigkeiten beteiligte Stellen auszuweiten. Die Kommission legt unter Berücksichtigung des Ergebnisses dieser Bewertung dem Europäischen Parlament und dem Rat im Rahmen der Überprüfung der Richtlinie (EU) 2015/2366 bis spätestens 17. Juli 2023 einen Bericht vor.

Auf der Grundlage dieses Überprüfungsberichts und nach Konsultation der ESA, der EZB und des ESRB kann die Kommission gegebenenfalls als Teil des Gesetzgebungsvorschlags, den sie gemäß Artikel 108 Unterabsatz 2 der Richtlinie (EU) 2015/2366 annehmen kann, einen Vorschlag unterbreiten, mit dem sichergestellt wird, dass alle Betreiber von Zahlungssystemen und alle an Zahlungsabwicklungstätigkeiten beteiligte Stellen einer angemessenen Überwachung unterliegen, wobei der bestehenden Überwachung durch die Zentralbank Rechnung zu tragen ist.

(3) Bis zum 17. Januar 2026 führt die Kommission nach Konsultation der ESA und des Ausschusses der Europäischen Aufsichtsstellen für Abschlussprüfer eine Überprüfung durch und legt — gegebenenfalls zusammen mit einem Gesetzgebungsvorschlag — dem Europäischen Parlament und dem Rat einen Bericht darüber vor, ob strengere Anforderungen an Abschlussprüfer und Prüfungsgesellschaften in Bezug auf die digitale operationale Resilienz angemessen sind, indem Abschlussprüfer und Prüfungsgesellschaften in den Geltungsbereich der vorliegenden Verordnung aufgenommen werden oder die Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates ([39]) geändert wird.

Abschnitt II

Änderungen

Artikel 59

Änderungen der Verordnung (EG) Nr. 1060/2009

Die Verordnung (EG) Nr. 1060/2009 wird wie folgt geändert:

1. Anhang I Abschnitt A Nummer 4 Unterabsatz 1 erhält folgende Fassung:

„Eine Ratingagentur verfügt über eine solide Verwaltung und Rechnungslegung, interne Kontrollmechanismen, effiziente Verfahren für die Risikobewertung sowie wirksame Kontroll- und Sicherheitsmechanismen für den Betrieb von IKT-Systemen gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*).

_____

(*) 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).“

2. Anhang III Nummer 12 erhält folgende Fassung:

„12. Die Ratingagentur verstößt gegen Artikel 6 Absatz 2 in Verbindung mit Anhang I Abschnitt A Nummer 4, wenn sie über keine solide Verwaltung und Rechnungslegung, keine internen Kontrollmechanismen, keine effizienten Verfahren für die Risikobewertung oder keine wirksamen Kontroll- und Sicherheitsmechanismen für den Betrieb von IKT-Systemen gemäß der Verordnung (EU) 2022/2554 verfügt oder wenn sie keine Entscheidungsprozesse oder keine Organisationsstruktur nach Maßgabe jener Nummer schafft oder unterhält.“

Artikel 60

Änderungen der Verordnung (EU) Nr. 648/2012

Die Verordnung (EU) Nr. 648/2012 wird wie folgt geändert:

1. Artikel 26 wird wie folgt geändert:

a) Absatz 3 erhält folgende Fassung:

„(3) Eine CCP muss dauerhaft über eine Organisationsstruktur verfügen, die Kontinuität und ein ordnungsgemäßes Funktionieren im Hinblick auf die Erbringung ihrer Dienstleistungen und Ausübung ihrer Tätigkeiten gewährleistet. Sie muss angemessene und verhältnismäßige Systeme, Ressourcen und Verfahren einsetzen, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) betrieben werden.

_____

(*) 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).“

([39]) Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates (ABl. L 157 vom 9.6.2006, S. 87).

b) Absatz 6 wird gestrichen;

2. Artikel 34 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Eine CCP hat eine angemessene Geschäftsfortführungsleitlinie sowie einen Notfallwiederherstellungsplan — der eine IKT-Geschäftsfortführungsleitlinie und IKT- Reaktions- und Wiederherstellungspläne umfasst, die nach der Verordnung (EU) 2022/2554 aufgestellt und umgesetzt werden — festzulegen, umzusetzen und zu befolgen, mit dem Ziel eine Aufrechterhaltung der Funktionen der CCP, eine rechtzeitige Wiederherstellung des Geschäftsbetriebs sowie eine Erfüllung der Pflichten der CCP zu gewährleisten."

b) Absatz 3 Unterabsatz 1 erhält folgende Fassung:

„(3) Um die einheitliche Anwendung dieses Artikels zu gewährleisten, erarbeitet die ESMA nach Anhörung der Mitglieder des ESZB Entwürfe für technische Regulierungsstandards, in denen der Mindestinhalt und die Anforderungen an die Geschäftsfortführungsleitlinie und an den Notfallwiederherstellungsplan, unter Ausschluss der IKT-Geschäftsfortführungsleitlinie und der Pläne für Notfallwiederherstellung, festgelegt werden."

3. Artikel 56 Absatz 3 Unterabsatz 1 erhält folgende Fassung:

„(3) Um die einheitliche Anwendung dieses Artikels zu gewährleisten, erarbeitet die ESMA Entwürfe für technische Regulierungsstandards, in denen die Einzelheiten des in Absatz 1 genannten Antrags auf Registrierung festgelegt werden, mit Ausnahme der Anforderungen im Zusammenhang mit dem IKT-Risikomanagement."

4. Artikel 79 Absätze 1 und 2 erhält folgende Fassung:

„(1) Ein Transaktionsregister ermittelt Quellen operationeller Risiken und minimiert diese Risiken durch die Entwicklung angemessener Systeme, Kontrollen und Verfahren, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2022/2554 betrieben werden.

(2) Ein Transaktionsregister hat eine angemessene Geschäftsfortführungsleitlinie und einen Notfallwiederherstellungsplan — einschließlich einer IKT-Geschäftsfortführungsleitlinie und IKT-Reaktions- und Wiederherstellungsplänen, die nach der Verordnung (EU) 2022/2554 eingerichtet werden — festzulegen, umzusetzen und zu befolgen, mit dem Ziel, die Aufrechterhaltung der Funktionen des Transaktionsregisters, die rechtzeitige Wiederherstellung des Geschäftsbetriebs sowie die Erfüllung der Pflichten des Transaktionsregisters zu gewährleisten."

5. Artikel 80 Absatz 1 wird gestrichen;

6. Anhang I Abschnitt II wird wie folgt geändert:

a) Die Buchstaben a und b erhalten folgende Fassung:

„a) Ein Transaktionsregister verstößt gegen Artikel 79 Absatz 1, wenn es nicht die Quellen betrieblicher Risiken ermittelt bzw. diese Risiken nicht durch die Entwicklung angemessener Systeme, Kontrollen und Verfahren, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2022/2554 betrieben werden, minimiert.

b) Ein Transaktionsregister verstößt gegen Artikel 79 Absatz 2, wenn es nicht eine angemessene Geschäftsfortführungsleitlinie und einen Notfallwiederherstellungsplan, die nach der Verordnung (EU) 2022/2554 eingerichtet werden, festlegt, umsetzt oder aufrechterhält, mit dem Ziel, die Aufrechterhaltung der Funktionen des Transaktionsregisters, die zeitnahe Wiederherstellung des Geschäftsbetriebs sowie die Erfüllung der Pflichten des Transaktionsregisters zu gewährleisten."

b) Buchstabe c wird gestrichen;

7. Anhang III wird wie folgt geändert:

a) Abschnitt II wird wie folgt geändert:

i) Buchstabe c erhält folgende Fassung:

„c) eine Tier 2-CCP verstößt gegen Artikel 26 Absatz 3, wenn sie nicht dauerhaft über eine Organisationsstruktur verfügt, die Kontinuität und ein ordnungsgemäßes Funktionieren im Hinblick auf die Erbringung ihrer Dienstleistungen und Ausübung ihrer Tätigkeiten gewährleistet, oder wenn sie keine angemessenen und geeigneten Systeme, Ressourcen und Verfahren einsetzt, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2022/2554 (DORA) betrieben werden;"

ii) Buchstabe f wird gestrichen.

b) in Abschnitt III erhält Buchstabe a folgende Fassung:

„a) eine Tier 2-CCP verstößt gegen Artikel 34 Absatz 1, wenn sie keine angemessene Geschäftsfortführungsleitlinie und keinen Reaktions- und Wiederherstellungsplan, die nach der Verordnung (EU) 2022/2554 eingerichtet werden, festlegt, umsetzt und befolgt, mit dem Ziel, eine Aufrechterhaltung der Funktionen der CCP, eine rechtzeitige Wiederherstellung des Geschäftsbetriebs sowie eine Erfüllung der Pflichten der CCP zu gewährleisten, wobei ein solcher Plan zumindest eine Wiederherstellung aller Transaktionen zum Zeitpunkt der Störung ermöglichen muss, sodass die CCP weiterhin zuverlässig arbeiten und die Abwicklung zum geplanten Termin vornehmen kann;“

Artikel 61

Änderungen der Verordnung (EU) Nr. 909/2014

Artikel 45 der Verordnung (EU) Nr. 909/2014 wird wie folgt geändert:

1. Absatz 1 erhält folgende Fassung:

„(1) Ein Zentralverwahrer ermittelt Quellen des internen und externen operationellen Risikos und hält deren Auswirkungen durch den Einsatz angemessener IKT-Tools, Verfahren und Strategien, die gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) eingerichtet und verwaltet werden, sowie durch alle anderen relevanten angemessenen Instrumente, Kontrollen und Verfahren für andere Arten operationeller Risiken, auch für alle von ihm betriebenen Wertpapierliefer- und -abrechnungssysteme, so gering wie möglich.

(*) 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).“

2. Absatz 2 wird gestrichen;

3. Absätze 3 und 4 erhalten folgende Fassung:

„(3) Für die von ihm erbrachten Dienstleistungen und jedes von ihm betriebene Wertpapierliefer- und -abrechnungssystem legt ein Zentralverwahrer eine angemessene Geschäftsfortführungsleitlinie sowie einen Notfallwiederherstellungsplan, einschließlich einer IKT-Geschäftsfortführungsleitlinie und IKT-Reaktions- und Wiederherstellungspläne, die gemäß der Verordnung (EU) 2022/2554 eingerichtet werden, fest, die er anwendet und befolgt, um bei Ereignissen, die ein beträchtliches Risiko einer Beeinträchtigung des Geschäftsbetriebs bergen, das Aufrechterhalten der Dienstleistungen, die rasche Wiederherstellung des Geschäftsbetriebs und die Erfüllung seiner Pflichten zu gewährleisten.

(4) Der Plan nach Absatz 3 muss eine Wiederherstellung aller Geschäfte und Positionen der Teilnehmer zum Zeitpunkt der Störung ermöglichen, damit die Teilnehmer eines Zentralverwahrers ihre Tätigkeiten in sicherer Weise fortsetzen und Lieferungen und Abrechnungen zum geplanten Termin vornehmen können; hierzu gehört auch die Vorsorge, dass kritische IT-Systeme nach der Störung wieder in Betrieb genommen werden können, so wie in Artikel 12 Absätze 5 und 7 der Verordnung (EU) 2022/2554 vorgesehen.“

4. Absatz 6 erhält folgende Fassung:

„(6) Ein Zentralverwahrer ermittelt, überwacht und managt die Risiken, die von wichtigen Teilnehmern an den von ihm betriebenen Wertpapierliefer- und -abrechnungssystemen sowie von Dienstleistern und Versorgungsbetrieben, anderen Zentralverwahrern oder anderen Marktinfrastrukturen für seinen Geschäftsbetrieb ausgehen könnten. Er unterrichtet die zuständige Behörde sowie die betreffenden Behörden auf Verlangen über alle solchermaßen ermittelten Risiken. Er unterrichtet die zuständige Behörde sowie die betreffenden Behörden ferner unverzüglich über alle Störfälle infolge dieser Risiken, die nicht im Zusammenhang mit dem IKT-Risiko auftreten.“

5. Absatz 7 Unterabsatz 1 erhält folgende Fassung:

„(7) Die ESMA arbeitet in enger Abstimmung mit den Mitgliedern des ESZB Entwürfe technischer Regulierungsstandards aus, in denen die operationellen Risiken nach den Absätzen 1 und 6 — mit Ausnahme von IKT-Risiken — sowie die Verfahren zur Prüfung, Bewältigung oder Minimierung dieser Risiken einschließlich der Geschäftsfortführungsleitlinien und der Notfallsanierungspläne nach den Absätzen 3 und 4 sowie der Verfahren zu ihrer Beurteilung präzisiert werden.“

Artikel 62

Änderungen der Verordnung (EU) Nr. 600/2014

Die Verordnung (EU) Nr. 600/2014 wird wie folgt geändert:

1. Artikel 27g wird wie folgt geändert:

   a) Absatz 4 erhält folgende Fassung:

   „(4) Ein APA muss die in der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) festgelegten Anforderungen in Bezug auf die Sicherheit von Netzwerk- und Informationssystemen erfüllen."

   _____

   (*) 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)."

   b) Absatz 8 Buchstabe c erhält folgende Fassung:

   „c) die konkreten organisatorischen Anforderungen nach den Absätzen 3 und 5."

2. Artikel 27h wird wie folgt geändert:

   a) Absatz 5 erhält folgende Fassung:

   „(5) Ein CTP muss die in der Verordnung (EU) 2022/2554 festgelegten Anforderungen in Bezug auf die Sicherheit von Netzwerk- und Informationssystemen erfüllen."

   b) in Absatz 8 erhält Buchstabe e folgende Fassung:

   „e) die konkreten organisatorischen Anforderungen nach Absatz 4."

3. Artikel 27i wird wie folgt geändert:

   a) Absatz 3 erhält folgende Fassung:

   „(3) Ein ARM muss die in der Verordnung (EU) 2022/2554 festgelegten Anforderungen in Bezug auf die Sicherheit von Netzwerk- und Informationssystemen erfüllen."

   b) Absatz 5 Buchstabe b erhält folgende Fassung:

   „b) die konkreten organisatorischen Anforderungen nach den Absätzen 2 und 4."

Artikel 63

Änderungen der Verordnung (EU) 2016/1011

In Artikel 6 der Verordnung (EU) 2016/1011 wird folgender Absatz angefügt:

„(6) Für kritische Referenzwerte verfügt ein Administrator über eine solide Verwaltung und Rechnungslegung, interne Kontrollmechanismen, effiziente Verfahren für die Risikobewertung sowie wirksame Kontroll- und Sicherheitsmechanismen für den Betrieb von IKT-Systemen gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*).

_____

(*) 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)."

Artikel 64

Inkrafttreten und Anwendung

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

Sie gilt ab dem 17. Januar 2025.

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

Geschehen zu Straßburg am 14. Dezember 2022.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident*
R. METSOLA	M. BEK