III

(Vorbereitende Rechtsakte)

EUROPÄISCHE ZENTRALBANK

STELLUNGNAHME DER EUROPÄISCHEN ZENTRALBANK

vom 4. Juni 2021

zu einem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors

(CON/2021/20)

(2021/C 343/01)

Einleitung und Rechtsgrundlage

Am 22., 23. bzw. 29. Dezember 2020 wurde die Europäische Zentralbank (EZB) vom Rat der Europäischen Union bzw. vom Europäischen Parlament um Stellungnahme zu einem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014 ([1]) (im Folgenden „Verordnungsvorschlag") und zu einem Vorschlag für eine Richtlinie zur Änderung der Richtlinien 2006/43/EG, 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 und (EU) 2016/2341 ([2]) (im Folgenden „vorgeschlagene Änderungsrichtlinie" und gemeinsam mit dem Verordnungsvorschlag als die „vorgeschlagenen Rechtsakte" bezeichnet) ersucht.

Die Zuständigkeit der EZB zur Abgabe einer Stellungnahme beruht auf Artikel 127 Absatz 4 und Artikel 282 Absatz 5 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), da die vorgeschlagenen Rechtsakte Bestimmungen enthalten, die in den Zuständigkeitsbereich der EZB fallen; hierzu gehören insbesondere die Festlegung und Durchführung der Geldpolitik, die Förderung des reibungslosen Funktionierens der Zahlungssysteme, die Mitwirkung bei der reibungslosen Durchführung der von den zuständigen Behörden auf dem Gebiet der Stabilität des Finanzsystems ergriffenen Maßnahmen und die Aufgaben der EZB im Zusammenhang mit der Aufsicht über die Kreditinstitute gemäß Artikel 127 Absatz 2 erster und vierter Gedankenstrich sowie Absätze 5 und 6 AEUV. Diese Stellungnahme wurde gemäß Artikel 17.5 Satz 1 der Geschäftsordnung der Europäischen Zentralbank vom EZB-Rat verabschiedet.

1. Allgemeine Anmerkungen

1.1 Die EZB begrüßt den Verordnungsvorschlag, mit dem die Cybersicherheit und die Betriebsstabilität des Finanzsektors verbessert werden sollen. Insbesondere begrüßt die EZB das Ziel des Verordnungsvorschlags, Hindernisse für den Binnenmarkt für Finanzdienstleistungen zu beseitigen und dessen Errichtung und Funktionieren zu verbessern, indem die Vorschriften für das Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT), die Berichterstattung, Prüfungen und das Risiko durch IKT-Drittanbieter harmonisiert werden. Darüber hinaus begrüßt die EZB das Ziel des Verordnungsvorschlags, etwaige sich überschneidende aufsichtsrechtliche Anforderungen bzw. Erwartungen, denen Finanzunternehmen derzeit nach Unionsrecht unterliegen, zu vereinheitlichen und zu harmonisieren.

1.2 Die EZB geht davon aus, dass der Verordnungsvorschlag in Bezug auf als Betreiber wesentlicher Dienste ermittelte Finanzunternehmen ([3]) einen sektorspezifischen Rechtsakt (*lex specialis*) im Sinne von Artikel 1 Absatz 7 der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([4]) (im Folgenden „NIS-Richtlinie") darstellt; daraus folgt, dass die Anforderungen des Verordnungsvorschlags grundsätzlich Vorrang vor der NIS-Richtlinie hätten. In der Praxis würden Finanzunternehmen, die als Betreiber wesentlicher Dienste ermittelt wurden, ([5]) u. a.

([1]) COM(2020) 595 final.
([2]) COM(2020) 596 final.
([3]) Siehe Artikel 1 Absatz 2 des Verordnungsvorschlags.
([4]) 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).
([5]) Siehe Artikel 5 der NIS-Richtlinie.

Vorfälle gemäß dem Verordnungsvorschlag und nicht gemäß der NIS-Richtlinie melden. Zwar begrüßt die EZB die Verringerung sich möglicherweise überschneidender Anforderungen für Finanzunternehmen im Bereich der Meldung von Vorfällen, doch sollte das Zusammenspiel zwischen dem Verordnungsvorschlag und der NIS-Richtlinie eingehender geprüft werden. Gemäß dem Verordnungsvorschlag könnten z. B. IKT-Drittanbieter ([6]) verpflichtet sein, den Empfehlungen der federführenden Aufsichtsinstanz ([7]) Folge zu leisten. Zugleich könnte derselbe IKT-Drittanbieter als Betreiber wesentlicher Dienste im Sinne der NIS-Richtlinie eingestuft und zur Befolgung verbindlicher Anweisungen der zuständigen Behörde verpflichtet sein. ([8]) Dieser Fall könnte dazu führen, dass der IKT-Drittanbieter verpflichtet wäre, Empfehlungen im Rahmen des Verordnungsvorschlags und verbindliche Anweisungen im Rahmen der NIS-Richtlinie zu befolgen, die einander widersprechen. Die EZB schlägt vor, dass die gesetzgebenden Organe der Union weiter prüfen, ob zwischen dem Verordnungsvorschlag und der NIS-Richtlinie ein Potenzial für Inkohärenzen besteht, das die Harmonisierung und Verringerung von sich überschneidenden und widersprüchlichen Anforderungen an Finanzunternehmen behindern könnte.

1.3 Die EZB geht ferner davon aus, dass gemäß dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 ([9]) (im Folgenden „NIS2-Richtlinienvorschlag“) „Beinahe-Vorfälle“ ([10]) Meldepflichten unterliegen werden. ([11]) Zwar wird in Erwägungsgrund 39 des NIS2-Richtlinienvorschlags auf die Bedeutung des Begriffs „Beinahe-Vorfälle“ Bezug genommen, es bleibt jedoch unklar, ob dadurch die Absicht zum Ausdruck gebracht wird, die in Artikel 2 des Verordnungsvorschlags aufgeführten Finanzunternehmen zur Meldung von Beinahe-Vorfällen zu verpflichten. In diesem Zusammenhang und unter Berücksichtigung der Tatsache, dass Beinahe-Vorfälle erst dann als solche eingestuft werden können, wenn sie eingetreten sind, würde die EZB eine rechtzeitige Unterrichtung über erhebliche Beinahe-Vorfälle entsprechend der aktuellen Praxis bei Cybervorfällen begrüßen. Die EZB schlägt vor, dass der Verordnungsvorschlag und der NIS2-Richtlinienvorschlag besser aufeinander abgestimmt werden sollten, um den genauen Umfang der Meldepflichten zu präzisieren, denen ein bestimmtes Finanzunternehmen im Rahmen dieser beiden unterschiedlichen, jedoch miteinander verbundenen Rechtsakte der Union unterliegen kann. Zugleich müssten „Beinahe-Vorfälle“ definiert werden, und es müssten Bestimmungen erarbeitet werden, die ihre Bedeutung präzisieren.

1.4 Die EZB begrüßt die Schaffung von Anreizen für den Austausch von Informationen zu Erkenntnissen über Cyberbedrohungen zwischen Finanzunternehmen auf freiwilliger Basis, um ihre Widerstandsfähigkeit gegenüber Cyberangriffen zu verbessern und zu stärken. Die EZB hat selbst die marktbasierte Cyber Information and Intelligence Sharing Initiative (Initiative für den Austausch von Informationen und Erkenntnissen über Cyberbedrohungen – CIISI-EU) gefördert und allen Interessierten Konzepte für die Auflegung und Förderung einer solchen Initiative zur Verfügung gestellt ([12]).

1.5 Die EZB unterstützt die Zusammenarbeit zwischen den für die Zwecke des Verordnungsvorschlags zuständigen Behörden, den Europäischen Aufsichtsbehörden (European Supervisory Authorities – ESA) und den Computer-Notfallteams (Computer Security Incident Response Teams – CSIRTs) ([13]). Es kommt entscheidend darauf an, Informationen auszutauschen, um die Betriebsstabilität in der Union zu gewährleisten, da der Informationsaustausch und die Zusammenarbeit zwischen den Behörden zur Prävention von Cyberangriffen und zur Eindämmung der Ausbreitung von IKT-Bedrohungen beitragen können. Unionsweit sollte ein gemeinsames Verständnis der IKT-Risiken gefördert und eine einheitliche Bewertung solcher Risiken sichergestellt werden. Es ist von allergrößter Bedeutung, dass die zuständigen Behörden ([14]) Informationen nur dann an die zentrale Anlaufstelle ([15]) und die nationalen CSIRTs weitergeben, wenn klar festgelegte Verfahren für die Klassifizierung und den Austausch von Informationen vorhanden sind, die mit angemessenen Garantien zur Gewährleistung der Vertraulichkeit einhergehen.

1.6 Schließlich würde die EZB die Einführung von Vorschriften über personenbezogene Daten und die Aufbewahrung von Daten im Rahmen des Verordnungsvorschlags begrüßen. Bei der Festlegung der Dauer der Aufbewahrungsfrist sollte berücksichtigt werden, welche Untersuchungen, Prüfungen, Informationsersuchen, Mitteilungen, Veröffentlichungen, Evaluierungen, Überprüfungen, Bewertungen sowie Überwachungs- oder Aufsichtspläne die zuständigen Behörden im

([6]) Siehe Artikel 3 Absatz 15 des Verordnungsvorschlags.
([7]) Siehe Artikel 31 Absatz 1 Buchstabe d des Verordnungsvorschlags.
([8]) Siehe Artikel 15 Absatz 3 der NIS-Richtlinie.
([9]) COM(2020) 823 final.
([10]) Ereignisse, die das Potenzial gehabt hätten, Schäden zu verursachen, deren vollständiger Eintritt jedoch verhindert wurde; siehe Erwägungsgrund 39 des NIS2-Richtlinienvorschlags.
([11]) Siehe Artikel 11 des NIS2-Richtlinienvorschlags.
([12]) Cyber Information and Intelligence Sharing Initiative (Initiative für den Austausch von Informationen und Erkenntnissen über Cyberbedrohungen – CIISI-EU), abrufbar auf der Website der EZB unter www.ecb.europa.eu.
([13]) Siehe Artikel 42 des Verordnungsvorschlags.
([14]) Siehe auch Artikel 11, 26 und 27 des NIS2-Richtlinienvorschlags.
([15]) Siehe Artikel 8 Absatz 3 der NIS-Richtlinie.

Rahmen ihrer jeweiligen Verpflichtungen und Aufgaben gemäß dem Verordnungsvorschlag durchzuführen bzw. zu erarbeiten haben. In diesem Zusammenhang wäre eine Aufbewahrungsfrist von 15 Jahren angemessen. Diese Aufbewahrungsfrist könnte je nach den Erfordernissen im Einzelfall verkürzt oder verlängert werden. In diesem Zusammenhang schlägt die EZB vor, dass die gesetzgebenden Organe der Union bei der Formulierung der einschlägigen Bestimmung über personenbezogene Daten und die Aufbewahrung von Daten auch den Grundsatz der Datenminimierung sowie die Weiterverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken berücksichtigen. ([16])

2. Spezifische Anmerkungen zur Überwachung sowie zur Verrechnung und Abwicklung von Wertpapieren

2.1 *Überwachungszuständigkeiten des ESZB und des Eurosystems*

2.1.1 In engem Zusammenhang mit dessen grundlegenden geldpolitischen Aufgaben sehen der AEUV und die Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank (im Folgenden „ESZB-Satzung“) vor, dass das Eurosystem die Überwachung der Verrechnungs- und Zahlungssysteme durchführt. Gemäß Artikel 127 Absatz 2 vierter Gedankenstrich AEUV und der entsprechenden Regelung in Artikel 3.1 vierter Gedankenstrich der ESZB-Satzung besteht eine der grundlegenden Aufgaben des Europäischen Systems der Zentralbanken (ESZB) darin, das reibungslose Funktionieren der Zahlungssysteme zu fördern. Im Rahmen der Wahrnehmung dieser grundlegenden Aufgabe können die EZB und die nationalen Zentralbanken Einrichtungen zur Verfügung stellen und kann die EZB Verordnungen erlassen, um effiziente und zuverlässige Verrechnungs- und Zahlungssysteme innerhalb der Union und im Verkehr mit dritten Ländern zu gewährleisten. ([17]) Im Einklang mit ihrer Überwachungsfunktion hat die EZB die Verordnung (EU) Nr. 795/2014 der Europäischen Zentralbank (EZB/2014/28) (im Folgenden „SIPS-Verordnung“) ([18]) erlassen. Mit der SIPS-Verordnung werden die Prinzipien für Finanzmarktinfrastrukturen vom April 2012 des Ausschusses für Zahlungsverkehrs- und Abrechnungssysteme (Committee on Payment and Settlement Systems – CPSS) und der Internationalen Organisation der Wertpapieraufsichtsbehörden (International Organization of Securities Commissions – IOSCO) ([19]) verbindlich umgesetzt, die rechtlich bindend sind und Großbetrags- und Massenzahlungssysteme von systemischer Bedeutung abdecken, die entweder von einer Zentralbank des Eurosystems oder von einem privaten Unternehmen betrieben werden. Im Rahmen des „Eurosystem Oversight Policy Framework“ ([20]) werden Zahlungsinstrumente als „integraler Bestandteil der Zahlungssysteme“ definiert und somit in den Anwendungsbereich der Überwachung durch das Eurosystem einbezogen. Der Rahmen für die Überwachung von Zahlungsinstrumenten wird gegenwärtig überprüft. ([21]) In diesem Rahmen wird ein Zahlungsinstrument (z. B. eine Karte, Überweisung, Lastschrift, E-Geld-Überweisung oder ein digitales Zahlungstoken ([22])) als personalisiertes Instrument (oder Reihe von Instrumenten) und/oder Verfahrensablauf definiert, das bzw. der zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister vereinbart wurde, um eine Wertübertragung ([23]) zu veranlassen.

2.1.2 In Anbetracht des Vorstehenden begrüßt die EZB, dass Systembetreiber im Sinne von Artikel 2 Buchstabe p der Richtlinie 98/26/EG des Europäischen Parlaments und des Rates ([24]), Zahlungssysteme (einschließlich solcher, die von Zentralbanken betrieben werden), Zahlverfahren und Zahlungsvereinbarungen mit Blick auf die Anwendung

([16]) Siehe Artikel 4 Buchstabe b und Artikel 13 der 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).

([17]) Siehe Artikel 22 der ESZB-Satzung.

([18]) Verordnung (EU) Nr. 795/2014 der Europäischen Zentralbank vom 3. Juli 2014 zu den Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme (EZB/2014/28) (ABl. L 217 vom 23.7.2014, S. 16).

([19]) Verfügbar auf der Website der Bank für Internationalen Zahlungsausgleich unter www.bis.org.

([20]) Überarbeitete Fassung des Rahmens der Überwachungspolitik des Eurosystems „Eurosystem Oversight Policy Framework“ (Juli 2016), abrufbar auf der Website der EZB unter www.ecb.europa.eu.

([21]) Siehe den überarbeiteten und konsolidierten Rahmen des Eurosystems für die Überwachung von elektronischen Zahlungsinstrumenten, -verfahren und -mechanismen von Oktober 2020 (PISA-Rahmen), abrufbar auf der Website der EZB unter www.ecb.europa.eu.

([22]) Ein digitales Zahlungstoken bezeichnet eine digitale Darstellung von Werten, die durch Forderungsansprüche oder Vermögenswerte, die anderweitig erfasst sind, unterlegt ist und die Übertragung von Werten zwischen den Endnutzern ermöglicht. Je nach dem zugrunde liegenden Design können digitale Zahlungstoken eine Wertübertragung vorsehen, ohne zwangsläufig einen zentralen Dritten einzubeziehen und/oder Zahlungskonten zu nutzen.

([23]) „Wertübertragung“: „Der vom Zahler oder im Namen des Zahlers oder vom Zahlungsempfänger ausgelöste Vorgang des Transfers von Geldbeträgen oder digitalen Zahlungstoken oder der Einzahlung oder Abhebung von Bargeld auf/von einem Nutzerkonto, ungeachtet etwaiger zugrunde liegender Verpflichtungen zwischen Zahler und Zahlungsempfänger. An der Übertragung können ein einzelner oder mehrere Zahlungsdienstleister beteiligt sein.“ Diese Definition von „Wertübertragung“ im Sinne des PISA-Rahmens weicht von der Begriffsbestimmung von Transfer von „Geldbeträgen“ gemäß der 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) ab. Eine „Wertübertragung“ im Zusammenhang mit einem „Zahlungsinstrument“ im Sinne der genannten Richtlinie kann sich nur auf eine Übertragung von „Geldbeträgen“ beziehen. Gemäß der genannten Richtlinie schließen „Geldbeträge“ keine digitalen Zahlungstoken ein, es sei denn, die Token können als E-Geld (oder, allerdings eher hypothetisch, als Giralgeld) eingestuft werden.

([24]) Richtlinie 98/26/EG des Europäischen Parlaments und des Rates vom 19. Mai 1998 über die Wirksamkeit von Abrechnungen in Zahlungs- sowie Wertpapierliefer- und -abrechnungssystemen (ABl. L 166 vom 11.6.1998, S. 45).

der oben genannten Überwachungsrahmen von dem Artikel, der den Geltungsbereich des Verordnungsvorschlags betrifft, ausgenommen sind. Aus diesen Gründen sollten die Zuständigkeiten des ESZB nach Maßgabe des AEUV und die Zuständigkeiten des Eurosystems gemäß der SIPS-Verordnung in den Erwägungsgründen des Verordnungsvorschlags eindeutig aufgeführt werden.

2.1.3 Ebenso begrüßt die EZB, dass IKT-Drittanbieter, die Aufsichtsrahmen unterliegen, die zur Unterstützung der in Artikel 127 Absatz 2 AEUV genannten Aufgaben eingerichtet wurden, von der Anwendung des im Verordnungsvorschlag vorgesehenen Aufsichtsrahmens ausgenommen sind. ([25]) In diesem Zusammenhang möchte die EZB betonen, dass die Zentralbanken des ESZB, wenn sie in ihrer Eigenschaft als Währungsbehörden handeln, ([26]) und das Eurosystem, wenn es Dienstleistungen über TARGET2, TARGET2-Securites (T2S) ([27]) und TARGET Instant Payment Settlement (TIPS) ([28]) erbringt, weder unter den Artikel fallen, der den Geltungsbereich des Verordnungsvorschlags betrifft, noch als IKT-Drittanbieter angesehen und somit potenziell als kritische IKT-Drittanbieter im Sinne des Verordnungsvorschlags eingestuft werden können. Das Eurosystem überwacht T2S im Zusammenhang mit seinem Mandat, effiziente und zuverlässige Verrechnungs- und Zahlungssysteme zu gewährleisten. Darüber hinaus hat die ESMA klargestellt, dass T2S kein kritischer Dienstleister ([29]) im Sinne der Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates ([30]) (im Folgenden „CSD-Verordnung“) ist. Infolgedessen werden die organisatorische und betriebliche Sicherheit, Effizienz und Stabilität von T2S durch den geltenden rechtlichen, regulatorischen und operativen Rahmen und die vereinbarten Governance-Regelungen von T2S und nicht durch die CSD-Verordnung gewährleistet.

2.1.4 Darüber hinaus deckt der Rahmen der Überwachungspolitik des Eurosystems ([31]) kritische Dienstleister wie die Society for Worldwide Interbank Financial Telecommunication (SWIFT) ab. SWIFT ist eine genossenschaftliche Gesellschaft mit beschränkter Haftung mit Sitz in Belgien, die sichere Nachrichtendienstleistungen auf internationaler Ebene anbietet. Die Nationale Bank van België/Banque Nationale de Belgique ist die federführende Überwachungsinstanz von SWIFT und führt auf der Grundlage einer Vereinbarung zur kooperativen Überwachung in Zusammenarbeit mit den anderen G10-Zentralbanken, einschließlich der EZB, die Überwachung von SWIFT durch. Die G10-Überwachungsinstanzen erkennen an, dass der Hauptschwerpunkt der Überwachung auf dem operationellen Risiko von SWIFT liegt, da dieses als die wichtigste Risikokategorie betrachtet wird, durch die SWIFT ein Systemrisiko für das Finanzsystem in der Union darstellen könnte. Die kooperative Überwachungsgruppe von SWIFT hat diesbezüglich ein spezifisches Bündel von Grundsätzen und einen Erwartungskatalog („High Level Expectations“) entwickelt, die auf SWIFT Anwendung finden, wie z. B. Risikoermittlung und -management, Informationssicherheit, Zuverlässigkeit und Resilienz, Technologieplanung und Kommunikation mit Anwendern. Die G10-Überwachungsinstanzen erwarten, dass SWIFT die Leitlinien „Guidance on cyber resilience for financial market infrastructures“ (Leitlinien über die Cyberresilienz für Finanzmarktinfrastrukturen) des Ausschusses für Zahlungsverkehr und Marktinfrastrukturen (Committee on Payment and Market Infrastructures – CPMI) und der Internationalen Organisation der Wertpapieraufsichtsbehörden (International Organization of Securities Commissions – IOSCO) ([32]) sowie andere internationale IKT-Sicherheitsstandards einhält, die zusammen über die im Verordnungsvorschlag festgelegten Anforderungen hinausgehen.

2.1.5 Es ist noch nicht geklärt, ob SWIFT und möglicherweise andere Dienstleister, die dem Rahmen der Überwachungspolitik des Eurosystems unterliegen, unter Umständen als IKT-Drittanbieter in den Anwendungsbereich des Verordnungsvorschlags fallen könnten, wenn sie Dienstleistungen erbringen sollten, die nicht von Artikel 127 Absatz 2 AEUV abgedeckt sind. Die EZB begrüßt daher nachdrücklich, dass Dienstleister, die bereits dem Rahmen der Überwachungspolitik des Eurosystems unterliegen, u. a. SWIFT, vom Anwendungsbereich des im Verordnungsvorschlag festgelegten Überwachungsrahmens ausgenommen sind.

([25]) Siehe Artikel 28 Absatz 5 des Verordnungsvorschlags.

([26]) Siehe Nummer 1.3 der Stellungnahme der Europäischen Zentralbank vom 19. Februar 2021 zu einem Vorschlag für eine Verordnung über Märkte für Kryptowerte und zur Änderung der Richtlinie (EU) 2019/1937 (CON/2021/4). Sämtliche Stellungnahmen der EZB sind auf EUR-Lex abrufbar.

([27]) Siehe Anhang IIa der Leitlinie EZB/2012/27 der Europäischen Zentralbank vom 5. Dezember 2012 über ein transeuropäisches automatisiertes Echtzeit-Brutto-Express-Zahlungsverkehrssystem (ABl. L 30 vom 30.1.2013, S. 1). Leitlinie EZB/2012/13 der Europäischen Zentralbank vom 18. Juli 2012 über TARGET2-Securities (ABl. L 215 vom 11.8.2012, S. 19); Beschluss EZB/2011/20 der Europäischen Zentralbank vom 16. November 2011 zur Festlegung detaillierter Regelungen und Verfahren für die Umsetzung der Zulassungskriterien für den Zugang von Zentralverwahrern zu TARGET2-Securities-Dienstleistungen (ABl. L 319 vom 2.12.2011, S. 117). Siehe ferner die T2S-Rahmenvereinbarung und die Collective Agreement (Gemeinsame Vereinbarung).

([28]) Siehe Anhang IIb der Leitlinie EZB/2012/27.

([29]) Siehe Artikel 30 Absatz 5 der 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) und Artikel 68 der Delegierten Verordnung (EU) 2017/392 der Kommission vom 11. November 2016 zur Ergänzung der Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für die Zulassung von und für aufsichtliche und operationelle Anforderungen an Zentralverwahrer (ABl. L 65 vom 10.3.2017, S. 48).

([30]) 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).

([31]) Überarbeitete Fassung des Rahmens der Überwachungspolitik des Eurosystems „Eurosystem Oversight Policy Framework“ (Juli 2016), abrufbar auf der Website der EZB unter www.ecb.europa.eu.

([32]) Verfügbar auf der Website der Bank für Internationalen Zahlungsausgleich unter www.bis.org.

2.2 *Zuständigkeiten des ESZB im Bereich der Wertpapierabwicklung*

2.2.1 Bei Zentralverwahrern handelt es sich um Finanzmarktinfrastrukturen (FMIs), die nach der CSD-Verordnung, in der die Anforderungen an die Lieferung und Abrechnung von Finanzinstrumenten und Vorschriften für die Organisation und Führung von Zentralverwahrern festgelegt werden, der strikten Regulierung und Beaufsichtigung durch unterschiedliche Behörden unterliegen. Darüber hinaus sollten Zentralverwahrer die Leitlinien über die Cyberresilienz für Finanzmarktinfrastrukturen des CPMI und der IOSCO beachten, die im Rahmen der Cyber Resilience Oversight Expectations for Financial Market Infrastructures (Oversight-Erwartungen im Hinblick auf die Cyberresilienz für Finanzmarktinfrastrukturen) operationalisiert wurden (Dezember 2018) ([33]). Neben den Aufsichtsbefugnissen, die den nationalen zuständigen Behörden (NCAs) im Rahmen der Verordnung über Zentralverwahrer übertragen sind, handeln die Mitglieder des ESZB als „betreffende Behörden" in ihrer Eigenschaft als für die Überwachung der von Zentralverwahrern betriebenen Wertpapierabwicklungssysteme zuständige Behörden, als Zentralbanken, welche die wichtigsten Währungen ausgeben, in denen Abrechnungen vollzogen werden, und als Zentralbanken, in deren Büchern die Geldseite von Geschäften abgerechnet wird. ([34]) Diesbezüglich wird in Erwägungsgrund 8 der Verordnung über Zentralverwahrer festgestellt, dass die vorgenannte Verordnung die Zuständigkeit der EZB und der nationalen Zentralbanken für die Gewährleistung effizienter und solider Clearing- und Zahlungssysteme innerhalb der Europäischen Union und im Verhältnis zu anderen Ländern nicht berühren sollte. In Erwägungsgrund 8 wird darüber hinaus festgestellt, dass die Verordnung über Zentralverwahrer dem Zugang der Mitglieder des ESZB zu den Informationen, die für die Erfüllung ihrer Aufgaben ([35]), einschließlich der Überwachung von Zentralverwahrern und anderen FMIs, ([36]) zweckdienlich sind, nicht entgegenstehen sollte.

2.2.2 Darüber hinaus fungieren die Mitglieder des ESZB häufig als Abwicklungsstellen für die Geldseite von Wertpapiergeschäften, und das Eurosystem bietet Zentralverwahrern Abwicklungsdienstleistungen über T2S an. Die Überwachung von T2S durch das Eurosystem steht im Zusammenhang mit dessen Mandat, effiziente und zuverlässige Verrechnungs- und Zahlungssysteme zu gewährleisten, während die für Zentralverwahrer zuständigen und betreffenden Behörden bestrebt sind, für deren reibungsloses Funktionieren, die Sicherheit und Effizienz der Abwicklung und das ordnungsgemäße Funktionieren der Finanzmärkte in ihrem jeweiligen Zuständigkeitsbereich zu sorgen.

2.2.3 Gemäß dem Verordnungsvorschlag ([37]) sind die Zentralbanken des ESZB nicht in die Erarbeitung technischer Standards in Bezug auf die Präzisierung von IKT-Risiken einbezogen. Ebenso werden die zuständigen Behörden nach dem Verordnungsvorschlag ([38]) nicht über IKT-bezogene Vorfälle unterrichtet. Die Zentralbanken des ESZB sollten in gleichem Maße einbezogen werden wie gegenwärtig in der CSD-Verordnung vorgesehen, und die betreffenden Behörden sollten über IKT-bezogene Vorfälle unterrichtet werden. Das Eurosystem ist die betreffende Behörde für alle Zentralverwahrer im Euro-Währungsgebiet und für mehrere andere Zentralverwahrer in der EU. Die Zentralbanken des ESZB müssten über IKT-bezogene Vorfälle unterrichtet werden, die für die Wahrnehmung ihrer Pflichten relevant sind, einschließlich der Überwachung von Zentralverwahrern und anderen FMIs. Die Risiken, denen Zentralverwahrer ausgesetzt sind, einschließlich IKT-Risiken, sind geeignet, das ordnungsgemäße Funktionieren von Zentralverwahrern zu gefährden. Daher sind IKT-Risiken für die betreffenden Behörden von Bedeutung, die einen vollständigen und detaillierten Überblick über diese Risiken erhalten sollten, um sie bewerten und Einfluss auf den Risikomanagementansatz der Zentralverwahrer nehmen zu können. Die im Verordnungsvorschlag festgelegten Anforderungen zu IKT-Risiken sollten nicht weniger restriktiv sein als die in der CSD-Verordnung und den derzeit geltenden technischen Regulierungsstandards vorgesehenen Anforderungen.

2.2.4 Darüber hinaus sollten die gesetzgebenden Organe der Union das Zusammenspiel zwischen dem Verordnungsvorschlag ([39]) und den technischen Regulierungsstandards zur Ergänzung der CSD-Verordnung klarstellen. Insbesondere ist nicht klar, ob ein Zentralverwahrer von der Verpflichtung zur Unterhaltung eines eigenen sekundären Bearbeitungsstandorts auszunehmen ist, wenn sein IKT-Drittanbieter einen solchen Standort unterhält. ([40]) Sollte ein Zentralverwahrer von dieser

([33]) Abrufbar auf der Website der EZB unter www.ecb.europa.eu.

([34]) Siehe Artikel 12 der Verordnung (EU) Nr. 909/2014.

([35]) Siehe auch Artikel 13, Artikel 17 Absatz 4 und Artikel 22 Absatz 6 der Verordnung (EU) Nr. 909/2014.

([36]) Siehe Nummer 7.3 der Stellungnahme der Europäischen Zentralbank vom 6. April 2017 zur Bestimmung Kritischer Infrastrukturen zum Zwecke der Sicherheit in der Informationstechnik (CON/2017/10); Nummer 7.2 der Stellungnahme der Europäischen Zentralbank vom 8. November 2018 zur Bestimmung wesentlicher Dienstleistungen und von deren Betreibern für die Zwecke der Sicherheit von Netzwerk- und Informationssystemen (CON/2018/47); Nummer 3.5.2 der Stellungnahme der Europäischen Zentralbank vom 2. Mai 2019 zur Sicherheit von Netzwerk- und Informationssystemen (CON/2019/17) und Nummer 3.5.2 der Stellungnahme der Europäischen Zentralbank vom 11. November 2019 zur Sicherheit von Netzwerk- und Informationssystemen (CON/2019/38).

([37]) Siehe Artikel 54 Absatz 5 des Verordnungsvorschlags und Artikel 45 Absatz 7 der Verordnung (EU) Nr. 909/2014.

([38]) Siehe Artikel 54 Absatz 4 des Verordnungsvorschlags und Artikel 45 Absatz 6 der Verordnung (EU) Nr. 909/2014.

([39]) Siehe Artikel 11 Absatz 5 des Verordnungsvorschlags.

([40]) Siehe Artikel 78 Absatz 3 der Delegierten Verordnung (EU) 2017/392 der Kommission vom 11. November 2016 zur Ergänzung der Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für die Zulassung von und für aufsichtliche und operationelle Anforderungen an Zentralverwahrer (ABl. L 65 vom 10.3.2017, S. 48).

Verpflichtung zur Unterhaltung eines sekundären Standorts ausgenommen sein, wäre die Rechtskraft dieser Anforderung unklar. Ebenso wird im Verordnungsvorschlag ([41]) auf eine Zeitvorgabe für die Wiederherstellung und auf Zeitvorgaben für die Wiederherstellungspunkte jeder Funktion ([42]) Bezug genommen, während in den einschlägigen technischen Regulierungsstandards in Bezug auf die für kritische Tätigkeiten von Zentralverwahrern festgelegten Sanierungszeiten zwischen kritischen Funktionen ([43]) und kritischen Tätigkeiten ([44]) unterschieden wird. Es sind weitere Klarstellungen und Überlegungen der gesetzgebenden Organe der Union hinsichtlich des Zusammenspiels zwischen dem Verordnungsvorschlag und den technischen Regulierungsstandards zur Ergänzung der CSD-Verordnung geboten, um dem Risiko widersprüchlicher Anforderungen zu begegnen. Schließlich sollte präzisiert werden, dass Ausnahmen, die Zentralverwahrern gewährt werden, die von bestimmten öffentlichen Stellen im Rahmen der CSD-Verordnung ([45]) verwaltet werden, nach Maßgabe des Verordnungsvorschlags verlängert werden.

2.3 *Zuständigkeiten des ESZB im Bereich der Wertpapierverrechnung*

2.3.1 Den Zentralbanken des ESZB wurde die Zuständigkeit im Bereich der Überwachung zentraler Gegenparteien (CCPs) übertragen. In dieser Hinsicht arbeiten die nationalen Zentralbanken des Eurosystems bei der Ausübung von Aufsichts- und Überwachungsfunktionen in Bezug auf CCPs häufig mit den jeweils zuständigen nationalen Behörden zusammen und gehören dem gemäß der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates ([46]) (European Market Infrastructure Regulation – EMIR, im Folgenden „EMIR") eingerichteten Kollegium der jeweiligen CCP an. Die einschlägigen Mitglieder des Eurosystems ([47]) gehören den EMIR-Kollegien im Rahmen ihrer Überwachungsfunktion an und vertreten das Eurosystem als emittierende Zentralbank für CCPs, bei denen der Euro eine der wichtigsten Währungen der abgerechneten Finanzinstrumente ist (und für Offshore-CCPs, die einen erheblichen Teil der Finanzinstrumente in Euro abrechnen). Die EZB ist die emittierende Zentralbank für zentrale Gegenparteien außerhalb des Euro-Währungsgebiets.

2.3.2 Gemäß dem Verordnungsvorschlag ([48]) sind die Zentralbanken des ESZB nicht in die Erarbeitung technischer Standards für die Präzisierung von IKT-Risiken eingebunden. Darüber hinaus wird im Verordnungsvorschlag ([49]) nicht auf die Anforderungen an die Zeitvorgabe für die Wiederherstellung und die Zeitvorgabe für die Wiederherstellungspunkte gemäß EMIR Bezug genommen. ([50]) Der vorgeschlagene Regulierungsrahmen sollte die in den geltenden Rechtsvorschriften vorgesehenen Anforderungen zu IKT-Risiken nicht aufweichen. Daher ist es von entscheidender Bedeutung, klare Zeitvorgaben für die Wiederherstellung und die Wiederherstellungspunkte festzulegen, um einen soliden Rahmen für die Fortführung des Geschäftsbetriebs zu schaffen. Die Beibehaltung spezifischer Zeitvorgaben für die Wiederherstellung und die Wiederherstellungspunkte ist zudem Teil der CPMI-IOSCO-Prinzipien für Finanzmarktinfrastrukturen. ([51]) Die derzeitige Bestimmung der EMIR-Verordnung sollte beibehalten und der Verordnungsvorschlag entsprechend angepasst werden. Die Zentralbanken des ESZB sollten in die Ausarbeitung von Rechtsvorschriften des Sekundärrechts sowie in weitere Klarstellungen und Überlegungen der gesetzgebenden Organe der Union zum Zusammenspiel zwischen dem Verordnungsvorschlag und den ergänzenden technischen Regulierungsstandards eingebunden werden, um dem Risiko widersprüchlicher oder sich überschneidender Anforderungen zu begegnen.

3. **Besondere Anmerkungen zu aufsichtsrechtlichen Aspekten**

3.1 Nach Maßgabe der Verordnung (EU) Nr. 1024/2013 des Rates ([52]) (im Folgenden „SSM-Verordnung") werden der EZB besondere Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute im Euro-Währungsgebiet sowie die Verantwortung für das wirksame und einheitliche Funktionieren des einheitlichen Aufsichtsmechanismus (Single Supervisory Mechanism – SSM) übertragen, innerhalb dessen spezifische Aufsichtsbefugnisse zwischen der EZB und den teilnehmenden NCAs aufgeteilt werden. Die EZB nimmt insbesondere die Aufgabe der Zulassung und des Entzugs der Zulassung aller Kreditinstitute wahr. Die EZB hat u. a. auch die Aufgabe zu gewährleisten, dass die einschlägigen Rechtsvorschriften der Union eingehalten werden, die Aufsichtsanforderungen an Kreditinstitute festlegen, einschließlich der Anforderung, über solide Regelungen für die Unternehmensführung, wie solide Risikomanagementverfahren und interne Kontrollmechanismen, zu verfügen. ([53]) Zu diesem Zweck werden der

([41]) Siehe Artikel 11 Absatz 6 des Verordnungsvorschlags.
([42]) Siehe Artikel 3 Absatz 17 des Verordnungsvorschlags.
([43]) Siehe Artikel 76 Absatz 2 Buchstaben d und e der Delegierten Verordnung (EU) 2017/392 der Kommission.
([44]) Siehe Artikel 78 Absätze 2 und 3 der Delegierten Verordnung (EU) 2017/392 der Kommission.
([45]) Siehe Artikel 1 Absatz 4 der Verordnung (EU) Nr. 909/2014.
([46]) 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).
([47]) Siehe Artikel 18 Absatz 2 Buchstaben g und h EMIR.
([48]) Siehe Artikel 53 Absatz 2 Buchstabe b und Absatz 3 des Verordnungsvorschlags sowie Artikel 34 Absatz 3 EMIR.
([49]) Siehe Artikel 53 Absatz 2 Buchstabe a des Verordnungsvorschlags.
([50]) Siehe Artikel 34 EMIR.
([51]) Siehe CPMI-IOSCO-Prinzipien für Finanzmarktinfrastrukturen, verfügbar auf der Website der Bank für Internationalen Zahlungsausgleich unter www.bis.org.
([52]) 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).
([53]) Siehe Artikel 4 Absatz 1 Buchstabe e und Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013.

EZB alle Aufsichtsbefugnisse übertragen, um in die Tätigkeit von Kreditinstituten einzugreifen, die für die Wahrnehmung ihrer Aufgaben erforderlich sind. Die EZB und die betreffenden NCAs sind daher die zuständigen Behörden, die gemäß der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates ([54]) (im Folgenden „Eigenkapitalverordnung") und der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates ([55]) (im Folgenden „Eigenkapitalrichtlinie") bestimmte Aufsichtsbefugnisse ausüben.

3.2 Der Verordnungsvorschlag sieht vor, dass das einheitliche Regelwerk und das Aufsichtssystem so weiterentwickelt werden sollten, dass sie auch die digitale Betriebsstabilität und die IKT-Sicherheit abdecken, indem die Mandate von Finanzaufsichtsbehörden, die mit der Überwachung und dem Schutz der Finanzstabilität und der Marktintegrität betraut sind, erweitert werden. ([56]) Ziel ist die Förderung eines umfassenden Rahmens für IKT oder operationelle Risiken durch die Harmonisierung der wichtigsten Anforderungen an die digitale Betriebsstabilität für alle Finanzunternehmen. ([57]) Mit dem Verordnungsvorschlag sollen insbesondere die Anforderungen mit Blick auf IKT-Risiken konsolidiert und verbessert werden, die bisher in den einzelnen Rechtsinstrumenten gesondert behandelt wurden. ([58])

3.3 Die Anforderungen mit Blick auf IKT-Risiken für den Finanzsektor verteilen sich derzeit auf eine Reihe von Rechtsakten der Union, darunter die Eigenkapitalrichtlinie, und nicht verbindliche Rechtsinstrumente (wie EBA-Leitlinien); sie sind vielfältig und bisweilen unvollständig. In einigen Fällen wurde das IKT-Risiko nur implizit als Teil des operationellen Risikos berücksichtigt, in anderen dagegen überhaupt nicht. Diesbezüglich sollte durch eine Angleichung des Verordnungsvorschlags und dieser Rechtsakte Abhilfe geschaffen werden. Zu diesem Zweck werden in der vorgeschlagenen Änderungsrichtlinie eine Reihe von Änderungen vorgelegt, die notwendig erscheinen, um für rechtliche Klarheit und Kohärenz in Bezug auf die Anwendung der verschiedenen Anforderungen an die digitale Betriebsstabilität zu sorgen. Die gegenwärtig in der vorgeschlagenen Änderungsrichtlinie empfohlenen Änderungen der Eigenkapitalrichtlinie ([59]) beziehen sich jedoch nur auf die Bestimmungen über Notfall- und Betriebskontinuitätspläne, ([60]), da sie anscheinend implizit als Grundlage für das IKT-Risikomanagement dienen.

3.4 Darüber hinaus sieht der Verordnungsvorschlag ([61]) vor, dass Finanzunternehmen, einschließlich Kreditinstituten, über interne Governance- und Kontrollrahmen verfügen, die eine wirksame und umsichtige Steuerung aller IKT-Risiken gewährleisten. Der Verordnungsvorschlag ([62]) sieht die Anwendung der darin festgelegten Anforderungen auf individueller und konsolidierter Ebene vor, ohne jedoch eine ausreichende Koordinierung mit den genannten sektorspezifischen Rechtsvorschriften zu gewährleisten. Schließlich ist im Verordnungsvorschlag ([63]) vorgesehen, dass unbeschadet der Bestimmungen über den im Verordnungsvorschlag genannten Aufsichtsrahmen für kritische IKT-Drittanbieter ([64]) die Einhaltung der darin festgelegten Pflichten bei Kreditinstituten durch die gemäß Artikel 4 der Eigenkapitalrichtlinie benannte zuständige Behörde sichergestellt wird, unbeschadet der besonderen Aufgaben, die der EZB durch die SSM-Verordnung übertragen wurden.

3.5 In Anbetracht des Vorstehenden geht die EZB davon aus, dass der Verordnungsvorschlag in Bezug auf Kreditinstitute und mit Ausnahme der Bestimmungen des Verordnungsvorschlags über den Aufsichtsrahmen für kritische IKT-Drittanbieter ([65]) einen aufsichtsrechtlichen internen Governance-Rahmen für das IKT-Risikomanagement festlegen soll, der in den allgemeinen internen Governance-Rahmen der Eigenkapitalrichtlinie integriert wird. Angesichts des aufsichtlichen Charakters des vorgeschlagenen Rahmens werden die zuständigen Behörden, die für die Aufsicht über die Einhaltung der in dem vorgeschlagenen Rahmen festgelegten Verpflichtungen zuständig sind, einschließlich der EZB, die für die Bankenaufsicht gemäß der SSM-Verordnung zuständigen Behörden sein.

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

([55]) 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).

([56]) Siehe Erwägungsgrund 8 des Verordnungsvorschlags.

([57]) Siehe Erwägungsgrund 11 des Verordnungsvorschlags.

([58]) Siehe Erwägungsgrund 12 des Verordnungsvorschlags.

([59]) Siehe Erwägungsgründe 4 und 5 der vorgeschlagenen Änderungsrichtlinie.

([60]) Siehe Artikel 85 der Eigenkapitalrichtlinie.

([61]) Siehe Artikel 4 Absatz 1 des Verordnungsvorschlags.

([62]) Siehe Artikel 25 Absätze 3 und 4 des Verordnungsvorschlags.

([63]) Siehe Artikel 41 des Verordnungsvorschlags.

([64]) Siehe Kapitel V Abschnitt II des Verordnungsvorschlags.

([65]) Siehe Kapitel V Abschnitt II des Verordnungsvorschlags.

3.6 Die gesetzgebenden Organe der Union könnten daher die folgenden Vorschläge zur Verbesserung der Klarheit und Koordinierung zwischen dem Verordnungsvorschlag und der Eigenkapitalrichtlinie in Erwägung ziehen. Erstens könnten die Anforderungen im Rahmen des Verordnungsvorschlags ausdrücklich als aufsichtsrechtlich eingestuft werden, wie dies u. a. in der CSD-Verordnung ([66]) erfolgt ist. Zweitens könnte der Wortlaut der Erwägungsgründe der vorgeschlagenen Änderungsrichtlinie ([67]) erweitert werden, da die Anforderungen des Verordnungsvorschlags über die reine Phase von Notfall- und Betriebskontinuitätsplänen hinausgehen. Governance-Maßnahmen zu IKT-Risiken fallen insgesamt in den allgemeineren Anwendungsbereich robuster Unternehmensführungsregelungen gemäß Artikel 74 der Eigenkapitalrichtlinie ([68]). Drittens sollte der Verordnungsvorschlag ([69]) dahin geändert werden, dass in den Erwägungsgründen auf die Zuständigkeit der EZB für die Aufsicht über Kreditinstitute gemäß AEUV und SSM-Verordnung hingewiesen wird. Viertens sollte der Verweis auf die Anwendung der darin festgelegten Anforderungen auf individueller und konsolidierter Ebene ([70]) überarbeitet werden, da teilkonsolidierte und konsolidierte Ebenen im Verordnungsvorschlag nicht definiert sind und bestimmte Arten von Vermittlern gemäß den einschlägigen Rechtsvorschriften nicht der konsolidierten Aufsicht unterliegen (z. B. Zahlungsinstitute). Darüber hinaus sollte sich die Anwendungsebene der Anforderungen des Verordnungsvorschlags ausschließlich aus den Rechtsvorschriften ergeben, die für jede Art von Finanzunternehmen gelten. Für Kreditinstitute ist ein eindeutiger Zusammenhang zwischen der Eigenkapitalrichtlinie und dem Verordnungsvorschlag vorgesehen, sodass die Anforderungen gemäß dem Verordnungsvorschlag automatisch auf individueller, teilkonsolidierter oder konsolidierter Basis gelten würden ([71]). Schließlich könnten die gesetzgebenden Organe der Union die Einführung einer Übergangsregelung in Erwägung ziehen, um den Zeitraum zwischen dem Inkrafttreten des Verordnungsvorschlags und dem Inkrafttreten der im Verordnungsvorschlag vorgesehenen technischen Regulierungsstandards zu überbrücken, da einige Vermittler, einschließlich Kreditinstituten, bereits Vorschriften über IKT-Risiken unterliegen, die für bestimmte Sektoren gelten und detaillierter sind als die allgemeinen Bestimmungen des Verordnungsvorschlags.

3.7 Der EZB wurde durch die SSM-Verordnung die Aufgabe übertragen, die Einhaltung der Anforderungen des Unionsrechts durch Kreditinstitute zu gewährleisten, denen zufolge diese über solide Risikomanagementverfahren und interne Kontrollmechanismen verfügen müssen. ([72]) Das bedeutet, dass die EZB sicherzustellen hat, dass die Kreditinstitute zur Beurteilung und Steuerung ihrer operationellen Risiken, einschließlich des Modellrisikos, sowie zur Absicherung gegen selten eintretende Ereignisse mit gravierenden Folgen auf Grundsätze und Verfahren zurückgreifen. Die Kreditinstitute müssen festlegen, was für die Zwecke dieser Grundsätze und Verfahren ein operationelles Risiko darstellt. ([73])

3.8 Im Juli 2017 verabschiedete der EZB-Rat auf der Grundlage eines Beschlussentwurfs des Aufsichtsgremiums nach Artikel 26 Absatz 8 und Artikel 6 Absatz 2 der SSM-Verordnung sowie Artikel 21 Absatz 1 der Verordnung (EU) Nr. 468/2014 der Europäischen Zentralbank (EZB/2014/17) ([74]) den SSM Cyber Incident Reporting Framework (SSM-Rahmen für die Meldung von Cybervorfällen, im Folgenden „Rahmen"). Der Rahmen besteht aus einem verbindlichen Informations- und/oder Meldeersuchen (an Kreditinstitute gerichtete Einzelbeschlüsse) auf der Grundlage von Artikel 10 der SSM-Verordnung. ([75]) In einigen Ländern wurde bereits ein Verfahren zur Meldung von Vorfällen eingeführt, nach dem Kreditinstitute verpflichtet sind, alle signifikanten Cybervorfälle ihren nationalen zuständigen Behörden zu melden. In diesen Ländern werden bedeutende Kreditinstitute Vorfälle weiterhin an die NCAs melden, die sie anschließend unverzüglich im Namen der beaufsichtigten Unternehmen an

([66]) Siehe Überschrift von Kapitel II Abschnitt 4 („Aufsichtsrechtliche Anforderungen") der CSD-Verordnung.
([67]) Siehe Erwägungsgrund 4 der vorgeschlagenen Änderungsrichtlinie.
([68]) Artikel 85 der Richtlinie 2013/36/EU ist eine bloße Spezifizierung. Siehe hierzu auch die Seiten 4, 11 und 37 der Leitlinien der Europäischen Bankenaufsichtsbehörde für das IKT- und Sicherheitsrisikomanagement vom 29. November 2019 (im Folgenden „EBA-Leitlinien"), in denen die allgemeine Rechtsgrundlage ausdrücklich in Artikel 74 der Richtlinie 2013/36/EU verortet wird.
([69]) Siehe Artikel 41 Absatz 1 des Verordnungsvorschlags.
([70]) Siehe Artikel 25 Absätze 3 und 4 des Verordnungsvorschlags.
([71]) Siehe auch Artikel 109 der Eigenkapitalrichtlinie.
([72]) Siehe Artikel 4 Absatz 1 Buchstabe e der SSM-Verordnung.
([73]) Siehe Artikel 85 der Eigenkapitalrichtlinie.
([74]) Verordnung (EU) Nr. 468/2014 der Europäischen Zentralbank vom 16. April 2014 zur Einrichtung eines Rahmenwerks für die Zusammenarbeit zwischen der Europäischen Zentralbank und den nationalen zuständigen Behörden und den nationalen benannten Behörden innerhalb des einheitlichen Aufsichtsmechanismus (SSM-Rahmenverordnung) (EZB/2014/17) (ABl. L 141 vom 14.5.2014, S. 1).
([75]) Insbesondere muss ein Cybervorfall (eine festgestellte mögliche Verletzung der Sicherheit des Informationssystems, ob böswillig oder versehentlich herbeigeführt) der EZB gemeldet werden, wenn mindestens eine der folgenden Bedingungen erfüllt ist: 1) Die potenziellen finanziellen Auswirkungen beziffern sich auf mindestens 5 Mio EUR bzw. 0,1 % des harten Kernkapitals, 2) der Vorfall wurde öffentlich bekannt gemacht oder hat Reputationsschäden zur Folge, 3) der Vorfall wurde außerhalb der regulären Berichterstattung an den Chief Information Officer eskaliert, 4) die Bank hat den Vorfall dem Computer Emergency Response Team bzw. dem Computer Security Incident Response Team, einer Sicherheitsbehörde oder der Polizei gemeldet, 5) es wurden Verfahren für die Wiederherstellung im Notfall und die Fortführung des Geschäftsbetriebs ausgelöst oder es wurde der Versicherung ein Cyberschadenfall gemeldet, 6) es wurde gegen gesetzliche oder aufsichtsrechtliche Anforderungen verstoßen oder 7) die Bank beschließt anhand interner Kriterien und Experteneinschätzungen (etwa in Bezug auf mögliche systemische Auswirkungen), die EZB-Bankenaufsicht zu informieren.

die EZB weiterleiten. Daher sind die oben genannten Beschlüsse auch an diese nationalen zuständigen Behörden gerichtet, damit diese Informationen auf der Grundlage des Rahmens an die EZB weitergeleitet werden. Die EZB unterstützt die Bemühungen der gesetzgebenden Organe der Union zur Harmonisierung und Vereinheitlichung u. a. der für Kreditinstitute geltenden Vorschriften und Pflichten in Bezug auf die Meldung von Vorfällen. Vor diesem Hintergrund ist die EZB bereit, den Rahmen gegebenenfalls im Lichte der späteren Verabschiedung des Verordnungsvorschlags zu ändern (und gegebenenfalls aufzuheben).

4. Spezifische Anmerkungen zum IKT-Risikomanagement, zur Meldung von Vorfällen, zur Prüfung der Betriebsstabilität und zum Risiko durch IKT-Drittanbieter

4.1 *IKT-Risikomanagement*

4.1.1 Die EZB begrüßt, dass mit dem Verordnungsvorschlag ein robuster und umfassender IKT-Risikomanagementrahmen eingeführt wird, der den CPMI-IOSCO-Leitlinien über die Cyberresilienz für Finanzmarktinfrastrukturen Rechnung trägt und eng an bewährte Verfahren angepasst ist, einschließlich der Oversight-Erwartungen im Hinblick auf die Cyberresilienz des Eurosystems für Finanzmarktinfrastrukturen.

4.1.2 Die EZB teilt die Auffassung, dass Finanzunternehmen bei jeder „wesentlichen Änderung" der Netz- und Informationssysteminfrastruktur, eine Risikobewertung durchführen müssen. ([76]) Allerdings enthält der Verordnungsvorschlag keine Definition des Begriffs „wesentliche Änderung", wodurch sich ein unerwünschter Spielraum für unterschiedliche Auslegungen durch Finanzunternehmen ergibt, der letztlich die Verwirklichung der Harmonisierungsziele des Verordnungsvorschlags beeinträchtigen könnte. Aus Gründen der Rechtssicherheit könnten die gesetzgebenden Organe der Union in Erwägung ziehen, eine Definition des Begriffs „wesentliche Änderung" in den Verordnungsvorschlag aufzunehmen.

4.1.3 Die EZB unterstützt generell den Ansatz, dass Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, einschlägige Kosten und Verluste melden, die durch IKT-Störungen und IKT-bezogene Vorfälle verursacht werden. ([77]) Um jedoch die Gesamteffizienz des Systems sicherzustellen und zu vermeiden, dass die zuständigen Behörden und Finanzunternehmen durch eine übermäßige Zahl von Berichten überfordert werden, könnte es hilfreich sein, die Einführung entsprechender, möglicherweise quantitativer Schwellenwerte durch die gesetzgebenden Organe der Union zu prüfen.

4.1.4 Die EZB erkennt an, dass Finanzunternehmen die Möglichkeit eingeräumt wird, die Überprüfung der Einhaltung der Anforderungen für das IKT-Risikomanagement nach Genehmigung durch die zuständigen Behörden an gruppeninterne oder externe Unternehmen zu delegieren. ([78]) Zugleich ist es wichtig, dass die gesetzgebenden Organe der Union klarstellen, wie die Genehmigung durch die zuständigen Behörden in Fällen erteilt würde, in denen ein Finanzunternehmen mehreren zuständigen Behörden untersteht. Dieser Fall könnte eintreten, wenn ein Finanzunternehmen ein Kreditinstitut, ein Anbieter von Krypto-Dienstleistungen und/oder ein Zahlungsdienstleister ist. Was schließlich die von Finanzunternehmen im Rahmen des Verordnungsvorschlags ([79]) durchzuführende Identifizierung und Klassifizierung betrifft, so würde es die EZB für die Zwecke der Klassifizierung der Informationsressourcen für umsichtig halten, dass Finanzunternehmen gemäß dem Verordnungsvorschlag auch verpflichtet werden, der Kritikalität solcher Informationsressourcen Rechnung zu tragen (d. h., ob sie kritische Funktionen unterstützen).

4.2 *Meldung von Vorfällen*

4.2.1 Die EZB begrüßt die im Verordnungsvorschlag beschriebenen Bemühungen zur Harmonisierung der Meldelandschaft für IKT-Vorfälle innerhalb der Union und die Arbeiten zur Zentralisierung der Berichterstattung über schwerwiegende IKT-bezogene Vorfälle. ([80]) Die Einführung eines harmonisierten Rahmens für die Meldung schwerwiegender IKT-bezogener Vorfälle ([81]) an die jeweils zuständigen Behörden würde den Meldeaufwand von Finanzunternehmen, einschließlich Kreditinstituten, grundsätzlich vereinheitlichen und harmonisieren. Die zuständigen Behörden würden von dem breiteren Spektrum der erfassten Vorfälle profitieren, das über die gegenwärtig von den bestehenden Rahmen abgedeckten Cybervorfälle hinausgeht. ([82]) Die künftige Verabschiedung des Verordnungsvorschlags würde eine Überprüfung und mögliche Aufhebung der bestehenden Rahmen erfordern, einschließlich des SSM-Rahmens für die Meldung von Cybervorfällen. Um jedoch eine wirkliche Vereinheitlichung und vollständige Angleichung aller Rahmen zu erreichen, muss unbedingt sichergestellt werden, dass der Anwendungsbereich der Bestimmungen über die Meldung von Vorfällen nach Maßgabe des Verordnungsvorschlags, einschließlich aller einschlägigen Definitionen, Schwellenwerte und Meldeparameter, vollständig an die

([76]) Siehe Artikel 7 Absatz 3 des Verordnungsvorschlags.
([77]) Siehe Artikel 10 Absatz 9 des Verordnungsvorschlags.
([78]) Siehe Artikel 5 Absatz 10 des Verordnungsvorschlags.
([79]) Siehe Artikel 7 des Verordnungsvorschlags.
([80]) Siehe Artikel 19 des Verordnungsvorschlags.
([81]) Siehe Artikel 3 Absatz 7, Artikel 17 und 18 des Verordnungsvorschlags.
([82]) Siehe z. B. den Rahmen.

einschlägigen Rahmen angeglichen wird. Insbesondere ist es von allergrößter Bedeutung, eine Angleichung zwischen dem Verordnungsvorschlag einerseits sowie der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates ([83]) (im Folgenden „PSD2“) und den EBA-Leitlinien für die Meldung schwerwiegender Vorfälle (im Folgenden „EBA-Leitlinien“) andererseits zu gewährleisten. Die vorgeschlagene Änderungsrichtlinie ([84]) sieht Änderungen der PSD2 in Bezug auf die Abgrenzung der Meldung von Vorfällen zwischen dem Verordnungsvorschlag und der PSD2 vor; diese würden vornehmlich Zahlungsdienstleister, die auch als Kreditinstitute zugelassen werden könnten, sowie die zuständigen Behörden betreffen. Das Verfahren zur Meldung von Sicherheitsvorfällen ist unklar, und es besteht eine potenzielle Überschneidung zwischen einigen der Vorfälle, die sowohl nach dem Verordnungsvorschlag als auch nach den EBA-Leitlinien gemeldet werden müssen.

4.2.2 Die Verfahren zur Meldung schwerwiegender Vorfälle gemäß dem Verordnungsvorschlag ([85]), der PSD2 bzw. den entsprechenden EBA-Leitlinien würden die Zahlungsdienstleister verpflichten, der jeweils zuständigen Behörde nach der Klassifizierung des Vorfalls einen Bericht über den Vorfall vorzulegen. In der Tat erfassen die ersten Meldungen nicht den wesentlichen Kern, die Ursache oder den Funktionsbereich, der von dem Vorfall betroffen ist, und Zahlungsdienstleister sind unter Umständen erst später in der Lage, derartige Unterscheidungen zu treffen, wenn detailliertere Informationen über den Vorfall vorliegen. Infolgedessen könnten erste Meldungen von Vorfällen im Rahmen sowohl des Verordnungsvorschlags als auch der EBA-Leitlinien vorgelegt werden, oder Zahlungsdienstleister können über einen einheitlichen Melderahmen entscheiden und ihre Meldungen zu einem späteren Zeitpunkt korrigieren. Die gleiche Unsicherheit (z. B. in Bezug auf die Hauptursache eines Vorfalls) kann sich im Hinblick auf die Zwischen- und Abschlussberichte ergeben. Dies würde erneut die Wahrscheinlichkeit einer parallelen Vorlage von Meldungen und Berichten an die zuständigen Behörden im Rahmen des Verordnungsvorschlags und der PSD2 erhöhen.

4.2.3 Einige Vorfälle, die unter Umständen als IKT-bezogene Vorfälle klassifiziert werden, können zudem Auswirkungen auf andere Bereiche haben und müssten daher gemäß den EBA-Leitlinien gemeldet werden. Dies kann der Fall sein, wenn ein Vorfall Auswirkungen aus IKT-Sicht hat, zugleich jedoch auch die Bereitstellung von Zahlungsdiensten unmittelbar und/oder andere funktionale Bereiche oder Kanäle außerhalb des IKT-Bereichs beeinträchtigt hat. Darüber hinaus könnte es Fälle geben, in denen es nicht möglich ist, zwischen operationellen und IKT-bezogenen Vorfällen zu unterscheiden. Ist dasselbe Finanzunternehmen ein bedeutendes Kreditinstitut und ein Zahlungsdienstleister, müsste es gemäß dem Verordnungsvorschlag den IKT-relevanten Vorfall zweimal melden, da es zwei zuständigen Behörden untersteht. Vor diesem Hintergrund sollte im Verordnungsvorschlag deutlicher zum Ausdruck kommen, wie das Zusammenspiel zwischen der PSD2 und den EBA-Leitlinien in der Praxis funktionieren soll. Im Interesse der Harmonisierung und Vereinheitlichung der Meldepflichten wäre es insbesondere wichtig, dass die gesetzgebenden Organe der Union Überlegungen zu den verbleibenden Fragen der doppelten Meldung anstellen und klären, ob der Verordnungsvorschlag einerseits und die PSD2 und die EBA-Leitlinien andererseits nebeneinander bestehen würden oder ob einheitliche Meldepflichten gelten sollten.

4.2.4. Gemäß dem Verordnungsvorschlag werden die zuständigen Behörden ([86]) verpflichtet, nach Eingang eines Berichts den Eingang der Meldung zu bestätigen und dem Finanzunternehmen schnellstmöglich alle erforderlichen Stellungnahmen oder Leitlinien zu übermitteln, um insbesondere Abhilfemaßnahmen auf Ebene des Unternehmens oder Möglichkeiten zur Minimierung nachteiliger Auswirkungen über Sektoren hinweg zu erörtern. Dies würde bedeuten, dass die zuständigen Behörden aktiv zur Bewältigung und Behebung von Vorfällen beitragen und zugleich die Reaktion eines beaufsichtigten Unternehmens auf kritische Vorfälle bewerten sollten. Die EZB betont, dass die Zuständigkeit und die Verantwortung für die Behebung und die Folgen eines Vorfalls allein und eindeutig bei dem betreffenden Finanzunternehmen verbleiben sollten. Die EZB schlägt daher vor, sich bei Stellungnahmen und Leitlinien auf aufsichtsrechtliche Stellungnahmen und Leitlinien zu beschränken, die von großer Wichtigkeit sind. Wenn die Stellungnahmen weiter gefasst würden, wären Experten mit umfangreichem Fachwissen erforderlich, die in der Regel nicht im Fachkräftepool der Aufsichtsbehörden zur Verfügung stehen.

4.3 *Prüfung der digitalen Betriebsstabilität*

4.3.1 Die EZB begrüßt die Anforderungen des Verordnungsvorschlags ([87]) an die Prüfung der digitalen Betriebsstabilität in Finanzunternehmen und das Erfordernis, dass jedes Unternehmen über ein eigenes Prüfungsprogramm verfügen muss. Im Verordnungsvorschlag ([88]) sind verschiedene Arten von Tests aufgeführt, die für Finanzunternehmen angezeigt sein können. Die Testarten sind nicht sehr klar, und einige Tests wie Kompatibilitätstests, Fragebögen oder

([83]) 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).

([84]) Siehe Artikel 7 Absatz 9 der vorgeschlagenen Änderungsrichtlinie.

([85]) Siehe Artikel 17 Absatz 3 des Verordnungsvorschlags.

([86]) Siehe Artikel 20 des Verordnungsvorschlags.

([87]) Siehe Artikel 21 und 22 des Verordnungsvorschlags.

([88]) Siehe Artikel 22 Absatz 1 des Verordnungsvorschlags.

szenariobasierte Tests können von ESA, zuständigen Behörden oder Finanzunternehmen unterschiedlich ausgelegt werden. Darüber hinaus gibt es auch keine Anhaltspunkte für die Häufigkeit der einzelnen Tests. Ein möglicher Ansatz könnte darin bestehen, dass im Verordnungsvorschlag allgemeine Prüfanforderungen festgelegt würden, wobei die Arten der Tests in technischen Regulierungs- und Durchführungsstandards genauer beschrieben würden.

4.3.2 Bedrohungsorientierte Penetrationstests (Threat-Led Penetration Testing – TLPT) sind ein leistungsfähiges Instrument, um Sicherheitsebenen und die Abwehrbereitschaft zu prüfen. Insofern befürwortet die EZB die Durchführung von TLPT durch Finanzunternehmen. Mit diesem Instrument werden nicht nur technische Maßnahmen geprüft, sondern auch Mitarbeiter und Prozesse. Die Ergebnisse dieser Tests können das Sicherheitsbewusstsein der höheren Führungsebene in den geprüften Unternehmen erheblich erhöhen. Das Europäische Rahmenwerk für ethisches Hacking auf Basis von Threat Intelligence (European Framework for Threat Intelligence-based Ethical Red Teaming – TIBER-EU) ([89]) und andere bereits außerhalb der Union verfügbare TLPT-Instrumente sind die wichtigsten Werkzeuge, mit denen die Unternehmen selbst ihre Aufstellung und ihre Abwehrmaßnahmen im Bereich der Cyberresilienz bewerten, testen, üben und verbessern können.

4.3.3 In den meisten Mitgliedstaaten, in denen TIBER-EU umgesetzt wurde, spielen Überwachungs- und Aufsichtsbehörden keine aktive Rolle bei der Umsetzung eines lokalen TIBER-XX-Programms, und das TIBER-Cyber-Team (TCT) ist in fast allen Fällen unabhängig von diesen Funktionen aufgestellt. Daher sollten erweiterte Prüfungen im Rahmen des Verordnungsvorschlags ([90]) mit Hilfe von TLPT eher als Instrument zur Stärkung des Finanzökosystems und zur Verbesserung der Finanzstabilität statt als rein aufsichtstechnisches Instrument umgesetzt werden. Darüber hinaus besteht kein Bedarf an der Entwicklung eines neuen Rahmens für die erweiterte Prüfung der Widerstandsfähigkeit gegenüber Cyberangriffen, da die Mitgliedstaaten TIBER-EU, , den einzigen solchen Rahmen in der EU, bereits weitgehend übernommen haben.

4.3.4 Die Anforderungen an Prüfer sollten nicht im verfügenden Teil des Verordnungsvorschlags enthalten sein, da sich der TLPT-Sektor noch weiterentwickelt und Innovationen möglicherweise durch die Festlegung spezifischer Anforderungen behindert werden. Die EZB vertritt jedoch die Auffassung, dass Finanzunternehmen, um bei der Durchführung von Tests ein hohes Maß an Unabhängigkeit zu gewährleisten, keine Prüfer einstellen oder beauftragen sollten, die von Finanzunternehmen ihrer eigenen Gruppe angestellt oder beauftragt werden oder die anderweitig den zu prüfenden Finanzunternehmen unterstehen und/oder unter deren Kontrolle stehen.

4.3.5 Um das Risiko einer Fragmentierung zu verringern und eine Harmonisierung zu gewährleisten, sollte im Verordnungsvorschlag ein TLPT-Rahmen vorgeschrieben werden, der auf den Finanzsektor in der gesamten Union Anwendung findet. Eine Fragmentierung kann sowohl für die zuständigen Behörden als auch für die Finanzunternehmen zu einer Erhöhung der Kosten und des Bedarfs an technischen, operativen und finanziellen Ressourcen führen. Diese höheren Kosten und Anforderungen können sich letztlich negativ auf die gegenseitige Anerkennung von Tests auswirken. Dieser Mangel an Harmonisierung und die sich daraus ergebenden Probleme im Zusammenhang mit der gegenseitigen Anerkennung sind besonders für Finanzunternehmen von entscheidender Bedeutung, die unter Umständen über mehrere Lizenzen verfügen und/oder in mehreren Mitgliedstaaten der Union tätig sind. Die technischen Regulierungs- und Durchführungsstandards, die im Rahmen des Verordnungsvorschlags für TLPT auszuarbeiten sind, sollten im Einklang mit TIBER-EU stehen. Darüber hinaus begrüßt die EZB die Möglichkeit, sich in Zusammenarbeit mit den ESA an der Ausarbeitung dieser technischen Regulierungs- und Durchführungsstandards zu beteiligen.

4.3.6 Die aktive Beteiligung der zuständigen Behörden an den Tests führt möglicherweise zu einem potenziellen Interessenkonflikt mit der anderen von ihnen ausgeübten Funktion, d. h. der Bewertung des Prüfungsrahmens des Finanzunternehmens. Vor diesem Hintergrund schlägt die EZB vor, alle Verpflichtungen der zuständigen Behörden in Bezug auf die Validierung von Unterlagen und die Ausstellung einer Bescheinigung für TLPT-Tests aus dem Verordnungsvorschlag zu streichen.

4.4 *Risiko durch IKT-Drittanbieter*

4.4.1 Die EZB begrüßt die Einführung eines umfassenden Katalogs zentraler Grundsätze und eines soliden Aufsichtsrahmens zur Ermittlung und Steuerung von IKT-Risiken, die von IKT-Drittanbietern ausgehen, unabhängig davon, ob diese zu derselben Finanzgruppe gehören. Im Hinblick auf eine wirksame Ermittlung und Steuerung von IKT-Risiken ist es jedoch wichtig, u. a. kritische IKT-Drittanbieter ordnungsgemäß zu identifizieren und zu klassifizieren. In dieser Hinsicht wird zwar die Verabschiedung delegierter Rechtsakte ([91]), die die Kriterien für die Zwecke der Klassifizierung ([92]) ergänzen, begrüßt, doch sollte die EZB vor dem Erlass solcher delegierter Rechtsakte konsultiert werden.

([89]) Abrufbar auf der Website der EZB unter www.ecb.europa.eu.
([90]) Artikel 23 und 24 des Verordnungsvorschlags.
([91]) Siehe Artikel 28 Absatz 3 des Verordnungsvorschlags.
([92]) Siehe Artikel 28 Absatz 2 des Verordnungsvorschlags.

4.4.2 Was die Struktur des Aufsichtsrahmens ([93]) anbelangt, so bedarf es weiterer Präzisierungen hinsichtlich der Rolle, die der Gemeinsame Ausschuss übernehmen soll. Zugleich begrüßt die EZB ihre Aufnahme in das Aufsichtsforum als Beobachterin, da diese Rolle der EZB den gleichen Zugang zu Unterlagen und Informationen bietet wie den stimmberechtigten Mitgliedern. ([94]) Die EZB möchte die gesetzgebenden Organe der Union darauf hinweisen, dass die EZB als Beobachterin einen Beitrag zur Arbeit des Aufsichtsforums leisten würde, und zwar sowohl in ihrer Eigenschaft als emittierende Zentralbank, die für die Überwachung der Marktinfrastrukturen zuständig ist, als auch als Aufsichtsbehörde für Kreditinstitute. Darüber hinaus stellt die EZB fest, dass sie nicht nur Beobachterstatus im Aufsichtsforum hat, sondern auch als zuständige Behörde Teil des gemeinsamen Untersuchungsteams sein wird. In diesem Zusammenhang könnten die gesetzgebenden Organe der Union weitere Überlegungen über die Zusammensetzung der gemeinsamen Untersuchungsteams ([95]) anstellen, um eine angemessen relevante Beteiligung der jeweils zuständigen Behörden zu gewährleisten. Zudem ist die EZB der Ansicht, dass die Höchstzahl der Teilnehmer an den gemeinsamen Untersuchungsteams erhöht werden sollte, wobei der Kritikalität, der Komplexität und dem Umfang der Dienste von IKT-Drittanbietern Rechnung zu tragen ist.

4.4.3 Die EZB stellt fest, dass die federführende Aufsichtsinstanz gemäß dem Verordnungsvorschlag möglicherweise verhindern kann, dass kritische IKT-Drittanbieter weitere Vereinbarungen über die Auftragsweitervergabe abschließen, wenn i) es sich bei dem ausgewählten Unterauftragnehmer um einen IKT-Drittanbieter oder einen IKT-Unterauftragnehmer mit Sitz in einem Drittland handelt und ii) die Vergabe von Unteraufträgen eine kritische oder wichtige Funktion des Finanzunternehmens betrifft. Die EZB möchte betonen, dass diese Befugnisse nur von der federführenden Aufsichtsinstanz im Zusammenhang mit Vereinbarungen über die Auftragsweitervergabe ausgeübt werden können, wenn ein kritischer IKT-Drittanbieter eine kritische oder wichtige Funktion an ein separates Rechtssubjekt mit Sitz in einem Drittland vergibt. Die EZB geht davon aus, dass die federführende Aufsichtsinstanz keine vergleichbaren Befugnisse ausüben könnte, um einen kritischen IKT-Drittanbieter daran zu hindern, kritische oder wichtige Funktionen des Finanzunternehmens an Einrichtungen dieses Anbieters auszulagern, die in einem Drittland ansässig sind. Es könnte beispielsweise der Fall sein, dass aus operationeller Sicht kritische Daten und/oder Informationen von Einrichtungen außerhalb des Europäischen Wirtschaftsraums (EWR) gespeichert oder verarbeitet werden können. In einem solchen Fall reichen die Befugnisse der federführenden Aufsichtsinstanz unter Umständen nicht aus, um die zuständigen Behörden in angemessener Weise zu bevollmächtigen, Zugang zu allen Informationen, Räumlichkeiten, Infrastrukturen und Mitarbeitern zu erhalten, die für die Wahrnehmung aller kritischen oder wichtigen Funktionen des Finanzunternehmens relevant sind. Um sicherzustellen, dass die zuständigen Behörden ihre Aufgaben ungehindert wahrnehmen können, schlägt die EZB vor, dass die federführende Aufsichtsinstanz die Befugnis erhalten sollte, auch die Nutzung von Einrichtungen außerhalb des EWR durch kritische IKT-Drittanbieter zu beschränken. Diese Befugnis könnte in den spezifischen Fällen ausgeübt werden, in denen keine Verwaltungsvereinbarungen mit den zuständigen Behörden von Drittländern bestehen, wie sie im Verordnungsvorschlag vorgesehen sind, ([96]) oder wenn die Vertreter der kritischen IKT-Drittanbieter nach dem Rahmenwerk des betreffenden Drittlands keine ausreichenden Zusicherungen hinsichtlich des Zugangs zu Informationen, Räumlichkeiten, Infrastrukturen und Mitarbeitern bieten, die für die Wahrnehmung von Überwachungs- oder Aufsichtsaufgaben erforderlich sind.

4.4.4 Schließlich könnte sich die Verpflichtung der zuständigen Behörden, die Empfehlungen der federführenden Aufsichtsinstanz ([97]) weiterzuverfolgen, als unwirksam erweisen, da die zuständigen Behörden möglicherweise keinen ganzheitlichen Überblick über die Risiken haben, die von den einzelnen kritischen IKT-Drittanbietern ausgehen. Darüber hinaus könnte es erforderlich sein, dass die zuständigen Behörden Maßnahmen gegen die von ihnen beaufsichtigten Finanzunternehmen ergreifen, wenn die kritischen IKT-Drittanbieter den Empfehlungen nicht nachkommen. Gemäß dem Verordnungsvorschlag ([98]) können die zuständigen Behörden von den von ihnen beaufsichtigten Finanzunternehmen verlangen, einen von einem kritischen IKT-Drittanbieter bereitgestellten Dienst vorübergehend auszusetzen oder laufende Verträge mit kritischen IKT-Drittanbietern zu kündigen. Es ist schwierig, den geplanten Follow-up-Prozess in konkrete Maßnahmen umzusetzen. Insbesondere ist nicht klar, ob ein beaufsichtigtes Finanzunternehmen in der Lage sein wird, einen Vertrag mit einem kritischen IKT-Drittanbieter auszusetzen oder zu kündigen. Dies ist darauf zurückzuführen, dass der kritische IKT-Drittanbieter für dieses Finanzunternehmen ein bedeutender Anbieter sein könnte oder diese Aussetzung oder Kündigung für das Finanzunternehmen mit vertraglichen oder sonstigen Kosten und Schäden verbunden sein könnte. Darüber hinaus unterstützt dieser Ansatz nicht die Konvergenz der Aufsicht, da die zuständigen Behörden dieselbe Empfehlung möglicherweise unterschiedlich auslegen. Dies könnte letztlich die angestrebte Harmonisierung und einen kohärenten Ansatz für die Überwachung von Risiken durch kritische IKT-Drittanbieter auf Unionsebene behindern. In Anbetracht der vorstehenden Ausführungen könnten die gesetzgebenden Organe der Union unter Berücksichtigung der durch die *Meroni*-Doktrin auferlegten Grenzen, die vom Gerichtshof der Europäischen Union in seinem Urteil in der Rechtssache ESMA ([99]) teilweise relativiert wurden, in Erwägung ziehen, den rechtlichen Aufsichtsinstanzen besondere Durchsetzungsbefugnisse gegenüber kritischen IKT-Drittanbietern zu übertragen.

([93]) Siehe Artikel 29 des Verordnungsvorschlags.
([94]) Siehe Artikel 29 Absatz 3 des Verordnungsvorschlags.
([95]) Siehe Artikel 35 des Verordnungsvorschlags.
([96]) Siehe Artikel 39 Absatz 1 des Verordnungsvorschlags.
([97]) Siehe Artikel 29 Absatz 4 und Artikel 37 des Verordnungsvorschlags.
([98]) Siehe Artikel 37 Absatz 3 des Verordnungsvorschlags.
([99]) Siehe Urteil des Gerichtshofs (Große Kammer) vom 22. Januar 2014, Vereinigtes Königreich Großbritannien und Nordirland gegen Europäisches Parlament und Rat der Europäischen Union, Rechtssache C-270/12.

Soweit die EZB Änderungen des Verordnungsvorschlags empfiehlt, sind spezielle Redaktionsvorschläge mit Begründung in einem gesonderten technischen Arbeitsdokument aufgeführt. Das technische Arbeitsdokument steht in englischer Sprache auf EUR-Lex zur Verfügung.

Geschehen zu Frankfurt am Main am 4. Juni 2021.

Die Präsidentin der EZB
Christine LAGARDE