Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Stellungnahme

Öffentliche Konsultation zu einem Rahmen für die Betriebsstabilität digitaler Systeme im Finanzdienstleistungssektor

Kontakt:
Berit Schimm
Telefon: +49 30 2021- 2111
Telefax: +49 30 2021-19-2100
E-Mail: b.schimm@bvr.de

Berlin, 17.3.2020

Federführer:
Bundesverband der Deutschen Volksbanken
und Raiffeisenbanken e. V.
Schellingstraße 4 | 10785 Berlin
Telefon: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-dk.de

Contribution ID: 05ca0133-e829-43db-9ad4-945ecd806e4f
Date: 17/03/2020 14:12:38

Öffentliche Konsultation zu einem Rahmen für die Betriebsstabilität digitaler Systeme im Finanzdienstleistungsbereich: den Finanzsektor in der EU widerstandsfähiger und sicherer gestalten

Mit * markierte Felder sind Pflichtfelder.

Einleitung

Diese Konsultation ist auch auf Englisch und Französisch verfügbar.

Digitalisierung und neue Technologien verändern ganz maßgeblich das europäische Finanzsystem und die Art und Weise, wie in Europa Finanzdienstleistungen für Unternehmen sowie Bürgerinnen und Bürger erbracht werden. Knapp zwei Jahre nach Annahme des FinTech-Aktionsplans durch die Kommission im Jahr 2018 sind die darin aufgeführten Maßnahmen weitgehend umgesetzt.

Um die Digitalisierung des Finanzsektors in Europa voranzubringen und gleichzeitig die damit einhergehenden Risiken angemessen zu regulieren, arbeiten die Dienststellen der Kommission vor dem Hintergrund des Auftragsschreibens an Exekutiv-Vizepräsidenten Dombrovskis auf eine neue Strategie zur Digitalisierung des Finanzsektors in der EU hin. Zu den Themen, über die besonders intensiv nachgedacht wird, gehören die Vertiefung des Binnenmarktes für digitale Finanzdienstleistungen, die Förderung eines datengestützten Finanzsektors in der EU unter Eindämmung der Risiken und Gewährleistung gleicher Wettbewerbsbedingungen, ein innovationsfreundlicherer Regulierungsrahmen für EU-Finanzdienstleistungen und die Stärkung der Betriebsstabilität digitaler Systeme[1] im Finanzsystem.

Diese öffentliche Konsultation und die parallel laufende öffentliche Konsultation zu Kryptoanlagen sind erste Schritte hin zu Initiativen, die die Kommission derzeit für diesen Bereich in Erwägung zieht. In den kommenden Monaten wird die Kommission möglicherweise auch Konsultationen zu weiteren Themen aus diesem Gebiet auf den Weg bringen.

Der Finanzsektor ist weltweit der größte Nutzer von Informations- und Kommunikationstechnologie (IKT) - auf ihn entfallen etwa ein Fünftel aller IKT-Ausgaben[2]. Seine Betriebsstabilität ist in hohem Maße von IKT abhängig. Diese Abhängigkeit wird - wie bei Finanzdienstleistungen, die von der Nutzung von Distributed-Ledger-Techniken und künstlicher Intelligenz profitieren, bereits der Fall - mit dem wachsenden Einsatz neuer Modelle, Konzepte oder Technologien weiter zunehmen. Gleichzeitig kann der verstärkte Einsatz künstlicher Intelligenz im Bereich der Finanzdienstleistungen die Notwendigkeit einer erhöhten Betriebsstabilität und dementsprechend der Gewährleistung einer angemessenen Aufsicht verursachen. Ob es sich nun um Online-Banking- oder Versicherungsdienstleistungen,

mobile Zahlungsanwendungen, digitale Handelsplattformen, Hochfrequenz-Handelsalgorithmen, digitale Clearing- und Abwicklungssysteme handelt - die heute angebotenen Finanzdienstleistungen basieren somit auf digitalen Technologien und Daten.

Die Abhängigkeit von IKT und Daten bringt neue Herausforderungen in Bezug auf die Betriebsstabilität mit sich. Die wachsende Digitalisierung von Finanzdienstleistungen in Verbindung mit dem Vorhandensein von hochwertigen Anlagen und (oft sensiblen) Daten macht das Finanzsystem für Betriebsstörungen und Cyberangriffe anfällig. Während der Finanzsektor wesentlich besser gegen IKT-Risiken (sowohl böswilliger als auch zufälliger Natur) abgesichert ist als andere Sektoren, wird das Risiko von Cyberangriffen in diesem Bereich dennoch dreimal so hoch eingeschätzt wie bei jedem anderen Bereich[3]. In den vergangenen Jahren haben die Häufigkeit und die Auswirkungen von Cyberzwischenfällen zugenommen, wobei Forscher die Gesamtkosten für die Weltwirtschaft auf zehn bis Hunderte von Milliarden Euro schätzen. Durch die zunehmende Digitalisierung des Finanzsektors wird sich dieser Trend beschleunigen. Die ständig wachsende Zahl und Professionalität von Cyberbedrohungen und IKT-Vorfällen im Finanzsektor machen deutlich, wie wichtig und dringend es ist, das Auftreten und die Auswirkungen dieser Risiken präventiv zu bekämpfen. Probleme im Hinblick auf die Betriebsstabilität, insbesondere IKT- und Sicherheitsrisiken, können ebenfalls ein Systemrisiko für den Finanzsektor bergen. Diese Probleme sollten als integraler Bestandteil des EU-Rechtsrahmens und des einheitlichen Regelwerks behandelt werden, mit dem die Wettbewerbsfähigkeit, Integrität, Sicherheit und Stabilität des europäischen Finanzsektors gewährleistet werden sollen.

Die Regulierung des EU-Finanzsektors erfolgt auf der Grundlage eines detaillierten und harmonisierten einheitlichen Regelwerks, durch das eine ordnungsgemäße Regulierung sowie gleiche Wettbewerbsbedingungen im gesamten Binnenmarkt gewährleistet werden und das in bestimmten Bereichen die Basis für die Beaufsichtigung bestimmter Finanzinstitute durch die EU-Organe bildet (z. B. die Beaufsichtigung von Kreditinstituten durch die Europäische Zentralbank bzw. den einheitlichen Aufsichtsmechanismus). Das Regelungswerk für Finanzdienstleistungen in der EU enthält bereits spezifische Vorschriften für IKT- und Sicherheitsrisiken sowie allgemeine Vorschriften für das Betriebsrisiko, aber diese Vorschriften sind in Bezug auf den Anwendungsbereich, die Granularität und die Spezifität fragmentiert. IKT- und Sicherheitsrisiken gehören zu den Hauptkomponenten des Betriebsrisikos, die die Aufsichtsbehörden im Rahmen ihres Mandats bewerten und überwachen sollten. Für die Erhaltung und Schaffung eines harmonisierten Ansatzes sowie für die Umsetzung internationaler Standards im Finanzsektor im Hinblick auf eine wirksamere Bewältigung von Problemen im Zusammenhang mit der Betriebsstabilität digitaler Systeme, die Schaffung von mehr Vertrauen und die Förderung digitaler Innovationen ist es wesentlich, dass die Finanzaufsichtsbehörden ihre Anstrengungen in einem harmonisierten und konvergenten Rahmen in den Mitgliedstaaten und den verschiedenen Teilen des Finanzsektors unternehmen. Sofern EU-Organe bestimmte Finanzinstitute direkt beaufsichtigen, wird dadurch auch sichergestellt, dass sie über die notwendigen, angemessen ausgestalteten Befugnisse verfügen.

Die EU hat Schritte in Richtung eines horizontalen Rahmens für Cybersicherheit unternommen, der eine Grundlage für alle Sektoren bildet[4]. Die IKT- und Sicherheitsrisiken, mit denen der Finanzsektor konfrontiert ist, sowie die Abwehrbereitschaft und der Grad an Integration dieses Sektors auf EU-Ebene rechtfertigen spezifische und fortgeschrittenere koordinierte Maßnahmen, die zwar auf dem horizontalen EU-Rahmen für Cybersicherheit aufbauen, aber erheblich über diesen hinausgehen und zur Erreichung eines höheren Maßes an Betriebsstabilität und Cybersicherheit beitragen, wie für den Finanzsektor vorausgesetzt wird.

Im Rahmen ihres Fintech-Aktionsplans hat die Europäische Kommission die Europäischen Aufsichtsbehörden (d. h. die Europäische Bankaufsichtsbehörde, die Europäische Wertpapier- und Marktaufsichtsbehörde und die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung) ersucht, eine finanzsektorübergreifende Erhebung der bestehenden Aufsichtspraktiken im Bereich IKT-Sicherheit und -Governance durchzuführen, die Aufstellung von Leitlinien in Betracht zu ziehen, um die Konvergenz der Aufsichtspraktiken zu fördern, und bei Bedarf eine fachliche Empfehlung an die Kommission im Hinblick auf eventuell erforderliche gesetzgeberische Verbesserungen zu richten. Die Kommission forderte die Europäischen Aufsichtsbehörden zudem auf, eine Kosten-/Nutzenanalyse für die Entwicklung eines kohärenten Testrahmens für die Cyberresilienz bedeutender Marktteilnehmer und Infrastrukturen im gesamten EU-Finanzsektor durchzuführen.

Hierauf aufbauend liegt der Schwerpunkt dieser öffentlichen Konsultation darauf, die Kommission über die Entwicklung eines potenziellen sektorübergreifenden EU-Rahmens für die Betriebsstabilität digitaler Systeme im

Finanzdienstleistungsbereich zu informieren. Die Konsultation zielt darauf ab, die Meinung von Interessengruppen insbesondere zu den folgenden Punkten zu erhalten:

- Stärkung der Betriebsstabilität digitaler Systeme im Finanzsektor, insbesondere in Bezug auf Aspekte im Zusammenhang mit IKT- und Sicherheitsrisiken;
- Hauptmerkmale eines verbesserten Rechtsrahmens, der sich auf mehrere Säulen stützt;
- Auswirkungen der potenziellen politischen Optionen.

Bestandsaufnahme der Interessengruppen

Es wurden die folgenden relevanten Interessengruppen ermittelt:

- Öffentliche Behörden: Regierungen der Mitgliedstaaten, nationale zuständige Behörden, alle relevanten Akteure im Bereich Finanzaufsicht, auch auf EU-Ebene (EU-Aufsichtsbehörden und andere relevante EU-Agenturen oder -Einrichtungen).
- Industrie, Wirtschaftsverbände, kleine und mittlere Unternehmen: Finanzdienstleister (z. B. Kreditinstitute, (Rück-)Versicherungsgesellschaften, Wertpapierfirmen, zentrale Gegenparteien, Zentralverwahrer, Transaktionsregister, Kreditratingagenturen, Wirtschaftsprüfungsgesellschaften, Vermögensverwalter, geregelte Märkte, Zahlungsdienstleister usw.), IKT-Dienstleister.
- Verbraucher, Nutzer von Finanzdienstleistungen und IKT-Diensten, Zivilgesellschaft.
- Wissenschaftliche Einrichtungen, gemeinnützige Organisationen und Denkfabriken.

Hintergrund der vorliegenden Konsultation

Auf internationaler Ebene besteht breiter politischer Konsens, dass Cyberrisiken im Finanzsektor durch die Verbesserung und Überprüfung der Cyberresilienz angegangen werden müssen. Cyberresilienz als Teil der breiter gefassten Arbeiten zur Betriebsstabilität von Finanzinstituten ist für viele Finanzaufsichts- und Regulierungsbehörden auf der ganzen Welt Priorität, wobei in verschiedenen internationalen Foren (z. B. Gruppe der Sieben (G7), Rat für Finanzstabilität, Basler Ausschuss für Bankenaufsicht (Basler Ausschuss), Ausschuss für Zahlungs- und Abrechnungssysteme der Zentralbanken der G10 und Internationale Organisation der Börsenaufsichtsbehörden (CPMI-IOSCO)) aktuell mehrere Arbeitsschwerpunkte aufgestellt wurden.

Auf EU-Ebene hat das Europäische Parlament die Kommission aufgefordert, „der Cybersicherheit im FinTech-Aktionsplan die höchste Priorität einzuräumen“[5]. Es betonte ferner die Notwendigkeit einer stärkeren Überwachung von Cyberrisiken, einer stärkeren Zusammenarbeit zwischen den zuständigen Behörden, eines besseren Austauschs von Informationen über Cyberbedrohungen zwischen den Marktteilnehmern sowie verstärkter Investitionen in wirksame Abwehrmaßnahmen gegen Cyberangriffe.

Der Fintech-Aktionsplan der Kommission umfasst Pläne zur Entwicklung eines speziellen Ansatzes in Bezug auf das Thema Cybersicherheit als Teil der Betriebsstabilität des EU-Finanzsektors. Die Entwicklung eines speziellen Ansatzes zur Verbesserung der Betriebsstabilität digitaler Systeme von Finanzinstituten erhält vor dem Hintergrund des vermehrten Abschlusses von Auslagerungsvereinbarungen und zunehmender Abhängigkeiten von Dritten (z. B. durch die Einführung der Cloud) noch größere Bedeutung. Wie im Fintech-Aktionsplan festgelegt, hat die Kommission mit mehreren politischen Maßnahmen reagiert, darunter die bevorstehende Aufstellung von Standardvertragsklauseln für Cloud-Vereinbarungen mit Unternehmen des Finanzsektors. Darüber hinaus haben die Europäischen Aufsichtsbehörden im April 2019 mit Blick auf künftige legislative Verbesserungen eine gemeinsame fachliche

Empfehlung herausgegeben. Ihre Bewertung hat eine Fragmentierung der IKT-Bestimmungen und der Sicherheits- bzw. Cybersicherheitsbestimmungen im Hinblick auf ihren Anwendungsbereich, ihre Granularität und ihre Spezifität in den EU-Rechtsvorschriften für Finanzdienstleistungen ergeben. Die Europäischen Aufsichtsbehörden forderten die Kommission daher auf, Gesetzesänderungen in den Bereichen IKT und Cybersicherheit für den EU-Finanzsektor vorzuschlagen, um die ermittelten Lücken und Unstimmigkeiten zu schließen bzw. zu beseitigen.

Insbesondere schlagen sie Gesetzesänderungen in vier Hauptbereichen vor: 1) Anforderungen bezüglich des IKT- und Sicherheitsrisikomanagements in den für den Finanzsektor geltenden Rechtsvorschriften, 2) Straffung der bestehenden Anforderungen bezüglich der Meldung von Sicherheitsvorfällen, 3) Einrichtung eines Rahmens für die Erprobung der Cyberresilienz und 4) Beaufsichtigung von für die Finanzinstitute tätigen Drittanbietern im IKT-Bereich.

In jüngerer Zeit haben die Mitgliedstaaten bei dem informellen Gespräch mit dem Rat (Wirtschaft und Finanzen) im September 2019 über die Widerstandsfähigkeit von Finanzinstituten gegen Cyberbedrohungen und „hybride" Bedrohungen auch auf die dringende Notwendigkeit hingewiesen, bessere Tests durchzuführen, mehr Informationen auszutauschen und die Koordinierung zwischen den Behörden zu verbessern.

In diesem Zusammenhang führt die Kommission eine öffentliche Konsultation durch, um Möglichkeiten zur Schaffung eines verbesserten Rahmens für die Betriebsstabilität digitaler Systeme im EU-Finanzsektor zu erkunden. Dieses Ziel könnte durch eine sektorübergreifende EU-Initiative für den Finanzsektor erreicht werden, die den Stärken und Besonderheiten der bestehenden internationalen, europäischen und nationalen Rahmen und Entwicklungen in den Bereichen IKT-Sicherheit und Risikomanagement Rechnung trägt.

---

[1] Mit dem im vorliegenden Dokument durchgängig verwendeten Begriff „Betriebsstabilität digitaler Systeme", der an dieser Stelle nicht genau definiert werden soll, ist die Fähigkeit eines Finanzinstituts zum Aufbau und zur Aufrechterhaltung seiner betrieblichen Integrität und des gesamten Spektrums an betrieblichen Kapazitäten gemeint, und zwar in Bezug auf alle digitalen und von der Datentechnologie abhängigen Komponenten, Werkzeuge und Prozesse, die vom Finanzinstitut zur Durchführung und Unterstützung seiner Geschäfte eingesetzt bzw. angewandt werden. Darin enthalten ist das IKT- und Sicherheitsrisikomanagement.

[2] Laut Statista beliefen sich die weltweiten IT-Ausgaben des Finanzsektors im Jahr 2014/2015 zusammengenommen auf 699 Mrd. USD und lagen damit deutlich über denen des Bereichs Fertigung und natürliche Ressourcen (477 Mrd. USD), der Medienbranche (429 Mrd. USD) oder des Regierungssektors (425 Mrd. USD). Die weltweiten IT-Gesamtausgaben im Jahr 2014/2015 wurden auf 3 734 Mrd. USD bzw. 3 509 Mrd. USD geschätzt, was darauf hindeutet, dass dabei fast jeder fünfte US-Dollar auf den Finanzsektor entfällt.

[3] Bericht des Europäischen Parlaments über Finanztechnologie: Einfluss der Technologie auf die Zukunft des Finanzsektors (2016/2243(INI)).

[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.

[5] Bericht des Europäischen Parlaments über Finanztechnologie: Einfluss der Technologie auf die Zukunft des Finanzsektors (2016/2243(INI)).

Hinweis: Um eine faire und transparente Konsultation zu gewährleisten, werden **nur die über diesen Online-Fragebogen eingegangenen Beiträge berücksichtigt** und in den zusammenfassenden Bericht einbezogen. Sollten Probleme bei der Beantwortung dieses Fragebogens auftreten oder sollten Sie dabei Hilfe benötigen, kontaktieren Sie bitte fisma-digital-operational-resilience@ec.europa.eu.

Weitere Informationen:

- zu dieser Konsultation
- zum Konsultationspapier
- zum Schutz personenbezogener Daten in dieser Konsultation

1. Angaben zu Ihrer Person

* Sprache meines Beitrags

- Bulgarisch
- Dänisch
- (•) Deutsch
- Englisch
- Estnisch
- Finnisch
- Französisch
- Griechisch
- Irisch
- Italienisch
- Kroatisch
- Lettisch
- Litauisch
- Maltesisch
- Niederländisch
- Polnisch
- Portugiesisch
- Rumänisch
- Schwedisch
- Slowakisch
- Slowenisch
- Spanisch
- Tschechisch
- Ungarisch

* In welcher Eigenschaft nehmen Sie an dieser Konsultation teil?

- Hochschule /Forschungseinrichtung
- (•) Wirtschaftsverband
- Unternehmen /Unternehmensverband
- Verbraucherorganisation
- EU-Bürger/in
- Umweltorganisation
- Nicht-EU-Bürger/in
- Nichtregierungsorganisation
- Öffentliche Behörde
- Gewerkschaft
- Sonstiges

* Vorname

Berit

* Nachname

Schimm

* E-Mail (wird nicht veröffentlicht)

b.schimm@bvr.de

* Name der Organisation

höchstens 255 Zeichen

Die Deutsche Kreditwirtschaft

* Größe der Organisation

- ○ Kleinstunternehmen (1 bis 9 Beschäftigte)
- ○ Kleinunternehmen (10 bis 49 Beschäftigte)
- ○ Mittleres Unternehmen (50 bis 249 Beschäftigte)
- ◉ Großunternehmen (250 oder mehr Beschäftigte)

Transparenzregisternummer

höchstens 255 Zeichen

Bitte prüfen Sie, ob Ihre Organisation im Transparenzregister eingetragen ist. Das Transparenzregister ist eine Datenbank, in der sich Organisationen, die Einfluss auf EU-Entscheidungsprozesse nehmen möchten, freiwillig eintragen lassen können.

52646912360-95

* Herkunftsland

Bitte geben Sie Ihr Herkunftsland oder das Ihrer Organisation an.

○ Afghanistan	○ Finnland	○ Litauen	○ Schweden
○ Ägypten	○ Frankreich	○ Luxemburg	○ Schweiz
○ Ålandinseln	○ Französische Süd- und Antarktisgebiete	○ Macao	○ Senegal
○ Albanien	○ Französisch-Guayana	○ Madagaskar	○ Serbien
○ Algerien	○ Französisch-Polynesien	○ Malawi	○ Seychellen
○ Amerikanische Jungferninseln	○ Gabun	○ Malaysia	○ Sierra Leone
○ Amerikanisch-Samoa	○ Gambia	○ Malediven	○ Simbabwe
○ Andorra	○ Georgien	○ Mali	○ Singapur
○ Angola	○ Ghana	○ Malta	○ Sint Maarten
○ Anguilla	○ Gibraltar	○ Marokko	○ Slowakei
○ Antarktis	○ Grenada	○ Marshallinseln	○ Slowenien
○ Antigua und Barbuda	○ Griechenland	○ Martinique	○ Somalia
○ Äquatorialguinea	○ Grönland	○ Mauretanien	○ Spanien
○ Argentinien	○ Guadeloupe	○ Mauritius	○ Sri Lanka

- Armenien
- Aruba
- Aserbaidschan
- Äthiopien
- Australien
- Bahamas
- Bahrain
- Bangladesch
- Barbados
- Belarus
- Belgien
- Belize
- Benin
- Bermuda
- Bhutan
- Bolivien
- Bonaire, St. Eustatius und Saba
- Bosnien und Herzegowina
- Botsuana
- Bouvetinsel
- Brasilien
- Britische Jungferninseln
- Britisches Territorium im Indischen Ozean
- Brunei
- Bulgarien
- Burkina Faso
- Burundi
- Cabo Verde
- Chile
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard und die McDonaldinseln
- Honduras
- Hongkong
- Indien
- Indonesien
- Insel Man
- Irak
- Iran
- Irland
- Island
- Israel
- Italien
- Jamaika
- Japan
- Jemen
- Jersey
- Jordanien
- Kaimaninseln
- Kambodscha
- Kamerun
- Kanada
- Kasachstan
- Mayotte
- Mexiko
- Mikronesien
- Moldau
- Monaco
- Mongolei
- Montenegro
- Montserrat
- Mosambik
- Myanmar /Birma
- Namibia
- Nauru
- Nepal
- Neukaledonien
- Neuseeland
- Nicaragua
- Niederlande
- Niger
- Nigeria
- Niue
- Nordkorea
- Nördliche Marianen
- Nordmazedonien
- Norfolkinsel
- Norwegen
- Oman
- Österreich
- Pakistan
- Palästina
- St. Barthélemy
- St. Helena, Ascension und Tristan da Cunha
- St. Kitts und Nevis
- St. Lucia
- St. Martin
- St. Pierre und Miquelon
- St. Vincent und die Grenadinen
- Südafrika
- Sudan
- Südgeorgien und Südliche Sandwichinseln
- Südkorea
- Südsudan
- Suriname
- Svalbard und Jan Mayen
- Syrien
- Tadschikistan
- Taiwan
- Tansania
- Thailand
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Trinidad und Tobago
- Tschad
- Tschechien
- Tunesien
- Türkei
- Turkmenistan

- ○ China
- ○ Clipperton
- ○ Cookinseln
- ○ Costa Rica
- ○ Côte d'Ivoire
- ○ Curaçao
- ○ Dänemark
- ○ Demokratische Republik Kongo
- ◉ Deutschland
- ○ Dominica
- ○ Dominikanische Republik
- ○ Dschibuti
- ○ Ecuador
- ○ El Salvador
- ○ Eritrea
- ○ Estland
- ○ Eswatini
- ○ Falklandinseln
- ○ Färöer
- ○ Fidschi
- ○ Katar
- ○ Kenia
- ○ Kirgisistan
- ○ Kiribati
- ○ Kleinere Amerikanische Überseeinseln
- ○ Kokosinseln (Keelinginseln)
- ○ Kolumbien
- ○ Komoren
- ○ Kongo
- ○ Kosovo
- ○ Kroatien
- ○ Kuba
- ○ Kuwait
- ○ Laos
- ○ Lesotho
- ○ Lettland
- ○ Libanon
- ○ Liberia
- ○ Libyen
- ○ Liechtenstein
- ○ Palau
- ○ Panama
- ○ Papua-Neuguinea
- ○ Paraguay
- ○ Peru
- ○ Philippinen
- ○ Pitcairninseln
- ○ Polen
- ○ Portugal
- ○ Puerto Rico
- ○ Réunion
- ○ Ruanda
- ○ Rumänien
- ○ Russland
- ○ Salomonen
- ○ Sambia
- ○ Samoa
- ○ San Marino
- ○ São Tomé und Príncipe
- ○ Saudi-Arabien
- ○ Turks- und Caicosinseln
- ○ Tuvalu
- ○ Uganda
- ○ Ukraine
- ○ Ungarn
- ○ Uruguay
- ○ Usbekistan
- ○ Vanuatu
- ○ Vatikanstadt
- ○ Venezuela
- ○ Vereinigte Arabische Emirate
- ○ Vereinigtes Königreich
- ○ Vereinigte Staaten
- ○ Vietnam
- ○ Wallis und Futuna
- ○ Weihnachtsinsel
- ○ Westsahara
- ○ Zentralafrikanische Republik
- ○ Zypern

* Tätigkeitsbereich oder Sektor (falls zutreffend):

mindestens 1 Antwort(en)

- ☐ Rechnungsführung
- ☐ Rechnungsprüfung
- ☑ Bankwesen
- ☐ Wertpapierfirma
- ☐ Zahlungsdienstleister
- ☐ Kreditratingagentur
- ☐ Versicherungen
- ☐ Altersversorgung
- ☐ Vermögensverwaltung (z. B. Hedgefonds, Private-Equity-Fonds, Risikokapitalfonds, Geldmarktfonds, Wertpapiere)

- ☐ Betrieb von Marktinfrastrukturen (z. B. zentrale Gegenparteien, Zentralverwahrer, Wertpapierbörsen)
- ☐ Soziales Unternehmertum
- ☐ Experte für Computer- und Netzsicherheit
- ☐ Akademische Einrichtungen
- ☑ Unternehmens-/Wirtschaftsverbände
- ☐ Sonstiges
- ☐ Nicht zutreffend

* Datenschutzeinstellungen für die Veröffentlichung

Die Kommission wird die Antworten auf diese öffentliche Konsultation veröffentlichen. Bitte geben Sie an, ob Ihre persönlichen Angaben veröffentlicht werden dürfen oder ob Sie anonym bleiben möchten.

- ○ **Anonym**
  Es werden lediglich die Art des Teilnehmers, das Herkunftsland und der Beitrag veröffentlicht. Alle anderen personenbezogenen Angaben (Name, Name und Größe der Organisation, Nummer im Transparenzregister) werden nicht veröffentlicht.
- ◉ **Öffentlich**
  Ihre personenbezogenen Angaben (Name, Name und Größe der Organisation, Nummer im Transparenzregister, Herkunftsland) werden zusammen mit Ihrem Beitrag veröffentlicht.

☑ Ich stimme den Bestimmungen zum Schutz personenbezogener Daten zu.

2. Bausteine für eine potenzielle EU-Initiative: zentrale Themen

---

Obwohl ein horizontaler EU-Rahmen für Cybersicherheit in verschiedenen Sektoren[6] besteht, wurden IKT- und Sicherheitsrisiken im Bereich der Finanzdienstleistungen im Regulierungs- und Aufsichtsrahmen der EU bisher nur zum Teil berücksichtigt. Der Schwerpunkt bei diesem Rahmen lag traditionell darauf, die finanzielle Belastbarkeit verschiedener Institutionen durch zusätzliche Kapital- und Liquiditätspuffer zu unterstützen und zum Schutz ihrer Nutzer und Kunden ihr Verhalten zu regulieren. Die Betriebsstabilität stand nicht so stark im Fokus, und noch weniger die Stärkung der Betriebsstabilität digitaler Systeme. Dazu gehören Risiken im Zusammenhang mit der zunehmenden Digitalisierung des Finanzbereichs sowie der Auslagerung und der daraus resultierenden Notwendigkeit einer verstärkten Cybervigilanz. Der horizontale EU-Rahmen für Cybersicherheit spiegelt die immer wichtigere Rolle von IKT im Finanzsektor und die damit verbundenen Risiken in Bezug auf die Betriebsstabilität einer Institution, das Vertrauen der Verbraucher und damit die Finanzstabilität nicht vollständig wider.

Anknüpfend an die von den drei Europäischen Aufsichtsbehörden im April 2019 vorgelegten Empfehlungen holt die Kommission die Ansichten der Interessengruppen zu folgenden Punkten ein:

- **Gezielte Verbesserungen der Anforderungen bezüglich des IKT- und Sicherheitsrisikomanagements** in den verschiedenen EU-Rechtsvorschriften für Finanzdienstleistungen. Diese Verbesserungen sind notwendig, um die Betriebsstabilität digitaler Systeme in allen wichtigen Finanzsektoren, die dem EU-Regulierungsrahmen für den Finanzbereich unterliegen, zu erhöhen. Sie könnten auf den bestehenden Anforderungen nach EU-

Recht aufbauen, bei denen international bereits vereinbarten Standards, Richtlinien oder Empfehlungen bezüglich der Betriebsstabilität (z. B. Richtlinien der Europäischen Aufsichtsbehörden, der G7, des Basler Ausschusses oder von CPMI-IOSCO), Rechnung getragen wird.[7]

- **Harmonisierung der Meldung von IKT-Vorfällen:** Die Vorschriften für die Meldung von Vorfällen sollten präzisiert und durch Bestimmungen zur Förderung einer besseren Überwachung und Analyse von IKT- und Sicherheitsrisiken ergänzt werden. Dabei könnte bestimmt werden, welche Vorfälle meldepflichtig sind, und es könnten diesbezügliche Erheblichkeitsschwellen und relevante Zeitrahmen festgelegt und gleichzeitig die Meldewege geklärt und die Vorlagen harmonisiert werden, um die Kohärenz und Benutzerfreundlichkeit zu erhöhen.

- **Entwicklung eines Rahmens für die Prüfung der Betriebsstabilität digitaler Systeme** in allen Finanzsektoren, der einen Mechanismus zur Vorausschätzung von Bedrohungen und zur Verbesserung der digitalen Betriebsbereitschaft von Finanzakteuren und Behörden vorsieht. Diese Bewertung könnte sich mit der Festlegung von Schlüsselanforderungen für Prüfungen der Betriebsstabilität digitaler Systeme unter Wahrung von Flexibilität und Verhältnismäßigkeit befassen, um den spezifischen Bedürfnissen der Finanzakteure entsprechend ihrer Größe, ihrer Komplexität und ihres Betriebsumfangs gerecht zu werden.

- Spezifische Regeln, die eine **bessere Aufsicht bestimmter kritischer IKT-Drittanbieter** ermöglichen, auf die regulierte Finanzinstitute angewiesen sind und an die sie Funktionen auslagern.

- Besondere Vorkehrungen **zur Förderung a) eines wirksamen Austauschs von Informationen** über IKT- und Sicherheitsbedrohungen zwischen den Finanzmarktteilnehmern und b) einer **besseren Zusammenarbeit** zwischen den öffentlichen Behörden.

---

[6] Richtlinie zur Netz- und Informationssicherheit und Verordnung (EU) 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (EU-Rechtsakt zur Cybersicherheit).

[7] Zum Beispiel die folgenden Dokumente: „Guidelines on ICT and security risk management“ (Leitlinien zum IKT- und Sicherheitsrisikomanagement) und „Guidelines on outsourcing arrangements“ (Leitlinien zu Auslagerungsvereinbarungen) der Europäischen Bankenaufsichtsbehörde, „G-7 Fundamental Elements of Cybersecurity for the Financial Sector“ (Grundelemente der Cybersicherheit für den Finanzsektor), „G-7 Fundamental Elements for Threat-Led Penetration Testing“ (Grundelemente für bedrohliche Penetrationstests) und „G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector“ (Grundelemente für das Cyber-Risikomanagement Dritter im Finanzsektor) sowie „Cyber-resilience: Range of practices“ (Cyberresilienz: Spektrum der Praktiken) des Basler Ausschusses, „Guidance on cyber resilience for financial market infrastructures“ (Leitfaden zur Cyber-Resilienz für Finanzmarktinfrastrukturen) von CPMI-IOSCO usw.

2.1 IKT- und Sicherheitsanforderungen

In ihrer gemeinsamen Empfehlung weisen die drei Europäischen Aufsichtsbehörden auf unterschiedliche, bisweilen inkonsistente Terminologie im gesamten Besitzstand in Bezug auf die Finanzdienstleistungen hin. Im Hinblick auf IKT- und Sicherheitsrisiken[8] scheint der EU-Besitzstand im Bereich der Finanzdienstleistungen zudem in Bezug auf den Detaillierungsgrad und die Spezifizität der entsprechenden Bestimmungen uneinheitlich zu sein. Gegenwärtig scheinen die Vorschriften zu IKT- und Sicherheitsrisiken (die manchmal implizit im Rahmen der Anforderungen in Bezug auf das Betriebsrisiko berücksichtigt und manchmal explizit im Zusammenhang mit den IKT-Anforderungen genannt werden) lückenhaft zu sein. Einige beaufsichtigte Finanzunternehmen unterliegen spezifischeren Anforderungen (z. B. im Rahmen der zweiten Zahlungsdiensterichtlinie, der Verordnung über Zentralverwahrer, der Verordnung über europäische Marktinfrastrukturen usw.)[9], während für andere Finanzunternehmen eher allgemeine oder gar keine Vorschriften gelten (z. B. neue Bankenrichtlinie/Eigenmittelverordnung, Richtlinie „Solvabilität II“, Richtlinie über Organismen für gemeinsame Anlagen in Wertpapiere/Richtlinie über die Verwaltung alternativer Investmentfonds usw.)[1]

[0]. Nicht alle EU-Rechtsvorschriften befassen sich mit dem gesamten Spektrum der Anforderungen bezüglich des IKT- und Sicherheitsrisikomanagements, die auf international vereinbarten Standards, Richtlinien oder Empfehlungen zum Cyber-Risikomanagement und zur Betriebsstabilität beruhen (z. B. G7, Baseler Ausschuss, CPMI-IOSCO usw.). Außerdem sind die Anforderungen nicht einheitlich zwischen den Rechtstexten der Stufe 1 (Verordnungen, Richtlinien) und der Stufe 2 (delegierte Rechtsakte und Durchführungsrechtsakte) über die verschiedenen Finanzsektoren verteilt.

Die drei Europäischen Aufsichtsbehörden verweisen insgesamt auf das Fehlen expliziter Bestimmungen über das IKT- und Sicherheitsrisikomanagement. Sie plädieren für ein klares Mindestmaß an Anforderungen im Bereich IKT-Sicherheit- und -Governance. Auf dieser Grundlage könnte eine Reihe von Verbesserungen im Zusammenhang mit den Anforderungen an das IKT-Risikomanagement erforderlich sein, um die Bereitschaft und Widerstandsfähigkeit aller wichtiger Finanzsektoren in Bezug auf Cyberangriffe zu stärken.

---

[8] Die Europäische Bankenaufsichtsbehörde hat kürzlich ihre „Guidelines on ICT and security risk management" (EBA/GL/2019/04) veröffentlicht, die für alle Institutionen, die in den Zuständigkeitsbereich der EBA fallen, gelten und darauf abzielen, die Widerstandsfähigkeit der Institutionen gegen IKT- und Sicherheitsrisiken zu stärken.

[9] Zweite Zahlungsdiensterichtlinie, Richtlinie (EU) 2015/2366, Verordnung über Zentralverwahrer, Verordnung (EU) Nr. 909/2014, Verordnung über die europäische Marktinfrastruktur (EMIR), Verordnung (EU) Nr. 648/2012.

[10] Eigenkapitalrichtlinie (CRD IV) (- Richtlinie 2013/36/EU, Eigenkapitalverordnung (CRR) - Verordnung (EU) Nr. 575/2013, Richtlinie „Solvabilität II" - Richtlinie 2009/138/EG, Richtlinie über Organismen für gemeinsame Anlagen in Wertpapieren (OGAW) - Richtlinie 2009/65/EG, Richtlinie über die Verwaltung alternativer Investmentfonds (AIFMD) - Richtlinie 2011/61/EU.

Frage 1 Sind Sie unter Berücksichtigung der engen Verflechtung des Finanzsektors, seiner weitreichenden Abhängigkeit von IKT-Systemen und des erforderlichen Vertrauens zwischen den Finanzakteuren der Meinung, dass alle Finanzunternehmen über einen Rahmen für das IKT- und Sicherheitsrisikomanagement verfügen sollten, der auf zentralen gemeinsamen Grundsätzen beruht?

- (●) Ja
- ( ) Nein
- ( ) Weiß ich nicht/keine Meinung/nicht relevant

Frage 1.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 1:

höchstens 5000 Zeichen

einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Initiativen in Richtung europaweit einheitlicher IT-Sicherheitsstandards und Harmonisierung der Aufsichtspraktiken sind grundsätzlich sinnvoll. Banken unterliegen bereits hohen Regulierungsstandards, eine zusätzliche Regulierung ist für Banken nicht erforderlich.
In Deutschland ist dies aufgrund der bestehenden gesetzlichen und regulatorischen Vorgaben u.a. die bankaufsichtlichen Anforderungen an die IT (BAIT) bereits gegeben. Zudem fordert das IT-Sicherheitsgesetz (Nationale Umsetzung der NIS-Richtlinie) die Umsetzung von IT-Sicherheitsmaßnahmen nach dem „Stand der Technik“.
Da sich Cyberkriminalität gezielt auf digitale Angriffspunkte richtet, gilt es, die Sicherheit von Finanzsystemen ganzheitlich zu regulieren und zu überwachen. Es ist es notwendig, dass alle Beteiligten Verantwortung für die IT-Sicherheit und die Cyberrisiken wahrnehmen. Einheitliche Vorgaben sollten sich sinnvoll in ein einheitliches Aufsichtskonzept gegenüber Finanzdienstleistern und Banken einfügen. Auch spezialgeschäftliche Vorgaben zur Informationssicherheit (Zahlungsverkehr, Wertpapiergeschäft, Risikomanagement) sollten in dieses Regelwerk eingefügt werden.
Die einheitlichen Vorgaben sollten ein Rahmenwerk bilden, in welchem alle Akteure Handlungsspielraum haben. Der Wettbewerb sollte nicht durch Maßnahmen-orientierte, detaillierte Vorgaben eingeschränkt werden. Vielmehr erscheint ein risikoorientiertes Rahmenwerk zielführend. Die Vorgaben und die Prüfungshandlungen sollten sich an internationalen Standards und Best Practices orientieren, um eine einheitliche Prüfungspraxis zu gewährleisten.

Frage 2 Wo war Ihre Organisation im Kontext des Risikomanagement-Zyklus bisher mit den meisten Schwierigkeiten, Lücken und Mängeln in Bezug auf die Robustheit und Ausfallsicherheit ihrer IKT-Infrastrukturen konfrontiert?

Angaben von 1 (nicht problematisch) bis 5 (äußerst problematisch)

	1 (überhaupt nicht problematisch)	2	3	4	5 (äußerst problematisch)	Weiß ich nicht/ keine Meinung/ nicht relevant
Identifizierung	○	○	○	○	○	○
Erkennung	○	○	○	○	○	○
Kapazität zum Schutz	○	○	○	○	○	○
Reaktion	○	○	○	○	○	○
Wiederherstellung	○	○	○	○	○	○
Lernen und Weiterentwicklung	○	○	○	○	○	○
Austausch von Bedrohungsinformationen mit anderen Finanzakteuren	○	○	○	○	○	○
Interne Koordinierung (innerhalb der Organisation)	○	○	○	○	○	○

Frage 2.1 Gibt es andere Phasen im Risikomanagement-Zyklus (oder ein anderes relevantes damit zusammenhängendes Element), in denen Ihre Organisation bisher mit den meisten Schwierigkeiten, Lücken und Mängeln k o n f r o n t i e r t w a r ?
Bitte geben Sie an, welche und erläutern Sie Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Die Fragen 2 bis 17 und 19 beziehen sich auf den Status Quo der Umsetzung von IKT-Anforderungen in einzelnen Instituten. Eine übergreifende Beantwortung dieser Fragen durch die Deutsche Kreditwirtschaft als Interessensvertretung der fünf deutschen kreditwirtschaftlichen Spitzenverbände ist nicht möglich.

Frage 2.2 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 2:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 3 Welches Maß an Beteiligung und/oder welche Art von Unterstützung/Maßnahmen hat der Vorstand (oder allgemeiner die Geschäftsleitung Ihrer Organisation) angeboten oder eingerichtet/vorgesehen, um den betreffenden IKT-Teams ein effektives IKT- und Sicherheitsrisikomanagement zu ermöglichen?

Angaben von 1 (keine Unterstützung/Maßnahme) bis 5 (hohe Unterstützung/äußerst umfassende Maßnahmen)

	1 (keine Unterstützung /Maßnahme)	2	3	4	5 (hohe Unterstützung/äußerst umfassende Maßnahmen)	Weiß ich nicht/ keine Meinung/ nicht relevant
Identifizierung	○	○	○	○	○	○
Erkennung	○	○	○	○	○	○
Kapazität zum Schutz	○	○	○	○	○	○
Reaktion	○	○	○	○	○	○
Wiederherstellung	○	○	○	○	○	○
Lernen und Weiterentwicklung	○	○	○	○	○	○
Austausch von Bedrohungsinformationen mit anderen Finanzakteuren	○	○	○	○	○	○
Interne Koordinierung (innerhalb der Organisation)	○	○	○	○	○	○

Frage 3.1 Gibt es irgendeine andere Art von Beteiligung, Unterstützung oder M a ß n a h m e ?
Bitte geben Sie an, welche und erläutern Sie Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 3.2 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 3 und heben Sie zusätzlich jede Art von Unterstützung und Maßnahmen hervor, die Ihrer Meinung nach vom Vorstand und der Geschäftsleitung geleistet bzw. ergriffen werden sollte:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 4 Wie erfolgt das IKT-Risikomanagement in Ihrer Organisation? Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 5 Welche wesentlichen Vorkehrungen, Strategien oder Maßnahmen haben Sie getroffen, um IKT-Risiken zu identifizieren und zu erkennen?

	Ja	Nein	Weiß ich nicht/ keine Meinung/ nicht relevant
Erstellen und pflegen Sie eine aktualisierte Abbildung der Geschäftsfunktionen, Rollen und unterstützenden Prozesse Ihrer Organisation?	○	○	○
Verfügen Sie über ein aktualisiertes Register/Inventar der unterstützenden IKT-Anlagen (z. B. IKT-Systeme, Mitarbeiter, Auftragnehmer, Dritte und Abhängigkeiten von anderen internen und externen Systemen und Prozessen)?	○	○	○
Nehmen Sie eine Klassifizierung der identifizierten Geschäftsfunktionen, unterstützenden Prozesse und Informationsbestände aufgrund ihrer Kritikalität vor?	○	○	○
Erstellen Sie eine Abbildung aller Zugriffsrechte und Berechtigungen und wenden Sie eine strenge rollenbasierte Zugriffspolitik an?	○	○	○
Führen Sie vor dem Einsatz neuer Informations- und Kommunikationstechnologien bzw. IKT-Modelle eine Risikobewertung durch?	○	○	○

Frage 5.1 Gibt es irgendeine andere Art von Vorkehrung, Politik oder Maßnahme?
Bitte geben Sie an, welche und erläutern Sie Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 5.2 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 5:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 6 Waren Sie Opfer von Cyberangriffen mit schwerwiegenden Folgen für Ihre Kunden oder Gegenparteien?

- Ja
- Nein
- Weiß ich nicht/keine Meinung/nicht relevant

Frage 6.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 6:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 7 Wie viele Cyberangriffe werden im Durchschnitt pro Jahr auf Ihre Organisation verübt? Wie viele davon haben Störungen in den kritischen Betriebsabläufen oder Diensten Ihrer Organisation verursacht bzw. könnten solche Störungen verursachen? Bitte erläutern Sie Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 8 Sind Sie der Ansicht, dass Ihre IKT-Systeme und -Werkzeuge geeignet sind sowie regelmäßig aktualisiert, getestet und überprüft werden, um Cyberangriffen oder IKT-Störungen standzuhalten und um ihre Betriebsstabilität zu gewährleisten? Welchen Unterschied stellen Sie in dieser Hinsicht zwischen internen und ausgelagerten IKT-Systemen und -Werkzeugen fest?

- Ja
- Nein
- Weiß ich nicht/keine Meinung/nicht relevant

Frage 8.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 8:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 9 Hat Ihre Organisation eine Cloud-Strategie entwickelt und eingeführt?

- Ja
- Nein
- Weiß ich nicht/keine Meinung/nicht relevant

Frage 9.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 9:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 11 Verfügen Sie über veraltete IKT-Systeme, die es im Hinblick auf erhöhte IKT-Sicherheitsanforderungen zu überprüfen gilt? Wie hoch wären die erforderlichen Investitionen (relativ oder absolut)?

- Ja
-

Nein

- Weiß ich nicht/keine Meinung/nicht relevant

Frage 11.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 11:

höchstens 5000 Zeichen

einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 12 Was sind Ihrer Meinung nach mögliche Ursachen für die Schwierigkeiten, denen Sie im Zusammenhang mit Cyberangriffen bzw. Beeinträchtigungen der IKT-Betriebsstabilität begegnet sind?

Angaben von 1 (nicht problematisch) bis 5 (äußerst problematisch)

	1 (überhaupt nicht problematisch)	2	3	4	5 (äußerst problematisch)	Weiß ich nicht/ keine Meinung/ nicht relevant
Komplexität der IKT-Umgebung	○	○	○	○	○	○
Probleme mit Altsystemen	○	○	○	○	○	○
Mangel an Analyseinstrumenten	○	○	○	○	○	○
Mangel an qualifiziertem Personal	○	○	○	○	○	○

Frage 12.1 Gibt es weitere mögliche Ursachen für die Schwierigkeiten, denen Sie im Zusammenhang mit Cyberangriffen bzw. Beeinträchtigungen der IKT-Betriebsstabilität begegnet sind? Bitte geben Sie an, welche und erläutern Sie Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 12.2 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 12:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 13 Verfügt Ihre Organisation Ihrer Meinung nach über hohe Verschlüsselungsstandards?

- Ja
- Nein
- Weiß ich nicht/keine Meinung/nicht relevant

Frage 13.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 13:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 14 Verfügen Sie über eine strukturierte Regelung für das IKT-Änderungsmanagement und regelmäßiges Patching sowie über eine detaillierte Backup-Regelung?

- Ja
- Nein
- Weiß ich nicht/keine Meinung/nicht relevant

Frage 14.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 14:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 15 Hat Ihre Organisation Ihrer Meinung nach Sicherheitsmaßnahmen für das Management und die Minderung von IKT- und Sicherheitsrisiken eingeführt und umgesetzt (z. B. Organisation und Governance, logische Sicherheit, physische Sicherheit, operative IKT-Sicherheit, Sicherheitsüberwachung, Überprüfung, Bewertung und Erprobung der Informationssicherheit und/oder Schulungen und Sensibilisierungsmaßnahmen im Bereich der Informationssicherheit)?

- Ja
- Nein
- Weiß ich nicht/keine Meinung/nicht relevant

Frage 15.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 15 und legen Sie dar, für welche Maßnahmen rechtliche Klarheit und Vereinfachung erforderlich wären:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 16 Wie schnell erfolgt in Ihrer Organisation im Durchschnitt die Wiederherstellung von Systemen nach IKT-Vorfällen, insbesondere nach schwerwiegenden bzw. groß angelegten Cyberangriffen? Gibt es in dieser Hinsicht Unterschiede je nach den Auswirkungen (Auswirkungen auf die Verfügbarkeit, auf die Vertraulichkeit oder eher auf die Integrität der Daten)? Soweit Sie es für erforderlich erachten, machen Sie bitte nähere Angaben.

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 17 Mit welchen Problemen haben Sie beim Versuch, eine schnelle Wiederherstellung der Systeme und die erforderliche Kontinuität bei der Durchführung Ihrer (kritischen) Betriebsfunktionen zu gewährleisten, am meisten zu kämpfen?

	Ja	Nein	Weiß ich nicht/ keine Meinung/ nicht relevant
Fehlen einer umfassenden Betriebskontinuitätspolitik und/oder von Wiederherstellungsplänen	○	○	○
Schwierigkeiten bei der Aufrechterhaltung kritischer/zentraler Geschäftsprozesse und der Verhinderung einer vollständigen Abschaltung	○	○	○
Probleme mit der internen Koordinierung (d. h. innerhalb Ihrer Organisation) bei der effektiven Umsetzung von Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs und zur Systemwiederherstellung	○	○	○
Fehlen von gemeinsamen Notfall-, Reaktions-, Wiederaufnahme-/Wiederherstellungsplänen für Cybersicherheitsszenarien (wenn mehrere Finanzakteure in Ihrem entsprechenden Ökosystem betroffen sind)	○	○	○

Keine Ex-ante-Ermittlung der genau benötigten Kapazitäten zur Sicherstellung der kontinuierlichen Systemverfügbarkeit	○	○	○
Schwierigkeiten der Einsatzteams, effektiv mit allen relevanten Teams (d. h. Geschäftsbereichen) in Ihrer Organisation zusammenzuarbeiten, um alle erforderlichen Maßnahmen zur Schadensbegrenzung und Wiederherstellung durchzuführen	○	○	○
Schwierigkeiten bei der Isolierung und Deaktivierung betroffener Informationssysteme	○	○	○

Frage 17.1 Gibt es weitere Probleme, mit denen Sie beim Versuch, eine schnelle Wiederherstellung der Systeme und die erforderliche Kontinuität bei der Durchführung Ihrer (kritischen) Betriebsfunktionen zu gewährleisten, zu kämpfen haben?
Bitte geben Sie an, welche und erläutern Sie Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 17.2 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 17:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 18 Was halten Sie davon, dass in der Gesetzgebung eine spezifische Zeit für die Notfallwiederherstellung (Recovery Time Objective) vorgesehen und auf den Wiederanlaufzeitpunkt nach einem Ausfall (Recovery Point Objective) verwiesen wird?
Soweit Sie es für erforderlich erachten, machen Sie bitte nähere Angaben.

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

RTO und RPO sind institutsspezifisch und risikoorientiert unter Berücksichtigung des Proportionalitätsprinzips festzulegen. Gesetzlich oder regulatorisch geforderte konkrete Vorgaben zu RTO und RPO sind nicht zielführend.

Frage 19 Durch welche Aktivitäten oder Maßnahmen setzen Sie aus Vorfällen gewonnene Erkenntnisse um und wie steigern Sie das Bewusstsein für Cybersicherheit in Ihrer Organisation?

	Ja	Nein	Weiß ich nicht/ keine Meinung/ nicht relevant
Fördern Sie die Mitarbeiterausbildung im Bereich IKT- und Sicherheitsrisiken durch regelmäßige Informationstreffen und/oder Schulungen?	○	○	○
Organisieren Sie regelmäßig spezielle Schulungen für die Mitglieder des Vorstands und der Geschäftsleitung?	○	○	○
Erhalten Sie vom Vorstand all die Unterstützung, die Sie für die Umsetzung wirksamer Programme zum Umgang mit Cybervorfällen und zur Verbesserung der Wiederherstellung benötigen?	○	○	○
Sorgen Sie dafür, dass die grundlegenden Ursachen identifiziert und beseitigt werden, um das wiederholte Auftreten von Vorfällen zu verhindern? Nehmen Sie Ex-post-Analysen der grundlegenden Ursachen von Cybersicherheitsvorfällen vor?	○	○	○

Frage 19.1 Gibt es andere Aktivitäten oder Maßnahmen, durch die Sie aus Vorfällen gewonnene Erkenntnisse umsetzen, oder Möglichkeiten, das Bewusstsein für Cybersicherheit in Ihrer Organisation zu erhöhen? Bitte geben Sie an, welche und erläutern Sie Ihre Ausführungen:

höchstens 5000 Zeichen

einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 19.2 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 19:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

2.2 Anforderungen bezüglich der Meldung von IKT- und Sicherheitsvorfällen

Die Europäischen Aufsichtsbehörden raten der Kommission, ein umfassendes, harmonisiertes System zur Meldung von IKT-Vorfällen für den Finanzsektor in Betracht zu ziehen. Dieses System sollte so konzipiert sein, dass Finanzunternehmen in der Lage sind, den zuständigen Behörden genaue und rechtzeitige Informationen zu melden, damit Firmen und Behörden IKT- und Sicherheitsrisiken ordnungsgemäß protokollieren, überwachen, analysieren und angemessen darauf reagieren und Betrug eindämmen können. Die Europäischen Aufsichtsbehörden schlagen vor, die Vorlagen, die Taxonomie und die Zeitrahmen nach Möglichkeit zu standardisieren. Schließlich sollte die Beziehung zu bestehenden Anforderungen bezüglich der Meldung von Vorfällen, z. B. gemäß der zweiten Zahlungsdiensterichtlinie oder der Verordnung über Zentralverwahrer sowie gemäß der Richtlinie zur Netz- und Informationssicherheit und der Datenschutz-Grundverordnung, geklärt werden.

Frage 20 Unterliegt Ihre Organisation derzeit Anforderungen bezüglich der Meldung von IKT- und Sicherheitsvorfällen?

- (●) Ja
- ( ) Nein
- ( ) Weiß ich nicht/keine Meinung/nicht relevant

Frage 20.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 20:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Banken unterliegen bereits zahlreichen Meldepflichten für kritische IT-Systeme insbesondere für die Zahlungsverkehrssysteme. Das bedeutet, dass ein einziger Vorfall dazu führen kann, dass Unternehmen bei verschiedenen Behörden Bericht erstatten müssen, wobei unterschiedliche Kriterien, Zeitpläne, Formulare und Kommunikationsmittel eingehalten werden müssen. Sowohl die PSD2-Richtlinie als auch das IT-Sicherheitsgesetz (Nationale Umsetzung der NIS-Richtlinie) beinhalten ein Meldewesen zu IT-Sicherheitsvorfällen. Die aus der PSD2-Richtlinie resultierenden Meldungen erfolgen an die nationale

Aufsicht und werden an die die EBA und die EZB weitergeleitet. SI-Banken müssen alle Cybersicherheitsvorfälle an die EZB melden. Zusätzlich haben EZB und Bundesbank im Zuge des Oversights der Zahlungssysteminfrastrukturen Meldepflichten installiert z.B. für Target 2. Meldungen gemäß IT-Sicherheitsgesetz gehen an die nationale Cybersicherheitsbehörde BSI. Darüber hinaus ergibt sich eine Meldepflicht für Vorfälle im Zusammenhang mit personenbezogenen Daten gemäß EU-DSGVO. Im Telekommunikationsbereich ergibt sich eine Meldepflicht an die nationale Aufsicht (Bundesnetzagentur) gemäß Telekommunikationsgesetz, aus eIDAS ein Meldewesen für Vertrauensdiensteanbieter.

Frage 21 Stimmen Sie zu, dass ein umfassendes und harmonisiertes EU-weites System zur Meldung von IKT- und Sicherheitsvorfällen für alle Finanzunternehmen konzipiert werden sollte?

- (●) Ja
- ( ) Nein
- ( ) Weiß ich nicht/keine Meinung/nicht relevant

Frage 21.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 21:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Eine Harmonisierung der Meldepflichten unter Berücksichtigung aller Beteiligten am Finanzsystem begrüßen wir, sofern bestehende Meldeverpflichtungen ersatzlos ersetzt und der Aufwand für die Meldenden dadurch effektiv reduziert wird. Dies wird sowohl den Unternehmen als auch den Aufsichtsbehörden zugutekommen, da Doppelarbeit und die Komplexität der Berichterstattung verringert werden, was wiederum den Aufsichtsbehörden konsistente und vergleichbare Daten im gesamten Finanzsektor zur Verfügung stellen wird. Eine solche Meldepflicht sollte alle Beteiligten umfassen und nicht auf Banken beschränkt sein, da Cyber-Kriminelle auch den gesamten Prozess im Blick haben. Die Meldungen sollten keine Einbahnstraße sein, sondern relevante Informationen zu Sicherheitsvorfällen von der Aufsicht an die Finanzdienstleister gegeben werden.

Frage 22 Wenn Sie Frage 21 mit „Ja“ beantwortet haben, erläutern Sie bitte, welche der folgenden Elemente harmonisiert werden sollten:

	Ja	Nein	Weiß ich nicht/ keine Meinung/ nicht relevant
Taxonomie der meldepflichten Vorfälle	(●)	( )	( )
Meldevorlagen	(●)	( )	( )
Meldezeitraum	(●)	( )	( )
Erheblichkeitsschwellen	(●)	( )	( )

Frage 22.1 Gibt es weitere Elemente des EU-weiten Systems für die Meldung von IKT-Vorfällen, die harmonisiert werden sollten? Bitte geben Sie an, welche und erläutern Sie Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 22.2 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 22:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Die Meldungen von sämtlichen IT-Sicherheitsvorfällen sollten nach einem einheitlichen Schema über einen einzigen Meldeweg erfolgen und über diesen Weg an alle ermächtigten Stellen weitergeleitet werden. Bei der Einführung von Erheblichkeitsschwellen für die Meldung von Vorfällen sind zu starre Schwellwerte z.B. absolute Werte zu vermeiden. Alternativ dazu empfehlen wir, die Wesentlichkeit auf regulatorische Vorgaben zu stützen und diese auf den eigenen Umfang, das eigene Wirkungsraster und das eigene kritische Dienstleistungsprofil anzuwenden.

Frage 23 Wie ausführliche sollte die Meldung von IKT- und Sicherheitsvorfällen sein? Bitte erläutern Sie, welche Informationen Sie für die Meldung als nützlich erachten und welche als unnötig angesehen werden können.
Soweit Sie es für erforderlich erachten, machen Sie bitte nähere Angaben.

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Der Detailgrad der Meldung sollte praxisrelevant ausgestaltet werden. Die bestehenden Meldeverpflichtungen sind ausreichend und sollten von unwichtigen Details befreit werden (z.B. Zwischenmeldungen bei den PSD2-Meldungen sind zu umfangreich).

Frage 24 Sollten alle Vorfälle meldepflichtig sein oder sollten Erheblichkeitsschwellen in Betracht gezogen werden, wobei kleinere Vorfälle zwar protokolliert und von dem betreffenden Unternehmen behandelt, der zuständigen Behörde jedoch nicht gemeldet werden müssten?

- ○ Ja
- ◉ Nein
- ○ Weiß ich nicht/keine Meinung/nicht relevant

Frage 24.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 24:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Die Meldungen sollten sich auf wesentliche Sicherheitsvorfälle beschränken, die die Versorgungssicherheit der Bevölkerung oder die Stabilität des Finanzwesens gefährden bzw. andere Banken betreffen können. Es sollte dann eine Meldung erfolgen, wenn auch ein relevanter und messbarer Schaden eingetreten ist, bzw. der Schaden absehbar eintreten wird. Dies kann helfen, die Diskussion über Schlussfolgerungen zu versachlichen.
Auf die Meldung kleinerer Vorfälle bzw. Betriebsstörungen sollte verzichtet werden, da dies wichtige Ressourcen des Unternehmens im Sicherheitsbereich bindet, ohne dass daraus ein angemessener Nutzen für die Widerstandsfähigkeit des Sektors oder die Erkenntnisse der Aufsichtsbehörden resultiert.

Frage 25 Welche Governance-Elemente rund um die Meldung von IKT- und Sicherheitsvorfällen wären erforderlich? Welchen zuständigen nationalen Behörden sollten IKT- und Sicherheitsvorfälle gemeldet werden? Oder sollte es eine einzige Behörde geben, die als zentrale EU-Drehscheibe bzw. -Datenbank fungiert? Soweit Sie es für erforderlich erachten, machen Sie bitte nähere Angaben.

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Generell sollten die Unternehmen bei einem Vorfall nur eine Meldung tätigen, anstatt an mehrere Behörden berichten zu müssen. Das Reporting sollte an einen Hub, der der jeweils für das Finanzinstitut zuständigen Fachaufsichtsbehörde zugeordnet ist, erfolgen. Bei Banken die der nationalen Aufsicht unterliegen, sollte die Meldung an einen nationalen Hub bei der Bankenaufsicht erfolgen. Über den Hub sollte über einen Mechanismus die Weiterleitung an alle weiteren berechtigten Stellen erfolgen - sowohl berechtigte EU-Institutionen als auch nationale Behörden.

Frage 26 Sollte ein ständiger Mechanismus zum Austausch von Vorfallsmeldungen zwischen den zuständigen nationalen Behörden eingerichtet werden?

- ○ Ja
- ○ Nein
- ◉ Weiß ich nicht/keine Meinung/nicht relevant

Frage 26.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 26:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Die Anzahl der beteiligten Stellen sollte so gering wie möglich sein, da Meldungen auch vertrauliche Informationen enthalten. Grundsätzlich ist ein Austausch der nationalen Stellen gegenüber einer Mehrfachmeldung zu bevorzugen. Wenn die gemeinsame Nutzung von Daten für notwendig und gerechtfertigt gehalten wird, sollte dies auf sichere Weise geschehen, z.B. möglicherweise durch die Schaffung anonymisierter und aggregierter Daten.

Frage 27 Welche Faktoren oder Anforderungen können derzeit die grenzübergreifende Zusammenarbeit und den Austausch von Informationen über IKT- und Sicherheitsvorfälle behindern? Soweit Sie es für erforderlich erachten, machen Sie bitte nähere Angaben.

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Vertraulichkeitsanforderungen können einen Austausch über Landesgrenzen behindern. Ebenso unterschiedliche Meldeanforderungen sowie unterschiedliche Taxonomien und Meldeformulare.

2.3. Rahmen für die Prüfung der Betriebsstabilität digitaler Systeme

---

Finanzinstitute müssen regelmäßig die Wirksamkeit ihrer Kapazitäten zur Prävention, Erkennung und Reaktion bewerten, um potenzielle Schwachstellen aufzudecken und zu beseitigen. In der Empfehlung der Europäischen Aufsichtsbehörden werden mehrere Instrumente zur Erreichung dieses Ziels genannt und es wird dazu geraten, einen mehrstufigen, schrittweisen Ansatz zu verfolgen, mit dem ein gemeinsamer Nenner für alle Finanzunternehmen

festgelegt und die Messlatte für die Betriebsstabilität digitaler Systeme im gesamten Finanzsektor in der EU angehoben wird. Kurzfristig empfehlen die Europäischen Aufsichtsbehörden, den Fokus auf die Prävention zu legen und dabei sicherzustellen, dass die Unternehmen eine grundlegende Bewertung der Schwachstellen in Bezug auf ihre Cybersicherheit durchführen. Mittelfristig schlagen die Europäischen Aufsichtsbehörden vor, für alle Finanzsektoren in der EU einen kohärenten Rahmen für die Prüfung der Cyberresilienz zu entwickeln und gemeinsame Leitlinien zu erstellen, die die gegenseitige Akzeptanz bzw. Anerkennung der Testergebnisse durch alle EU-Aufsichtsinstanzen zum Ergebnis haben könnten.

Im Allgemeinen kann die Prüfung der Widerstandsfähigkeit gegenüber Cyberangriffen ein äußerst wirksames Instrument darstellen, wenn es darum geht, fehlende Aspekte der IKT- und Sicherheitspolitik zu ermitteln, reales Feedback über einige der am stärksten gefährdeten Wege in die Systeme und Netze des Unternehmens zu geben und das Bewusstsein für die IKT-Sicherheit und -Widerstandsfähigkeit innerhalb des Finanzunternehmens zu schärfen. Zudem kann dadurch ein Beitrag zur Schaffung eines Binnenmarkts für Informations- und Testanbieter geleistet werden.

Werden in den einzelnen Mitgliedstaaten unterschiedliche, durch regulatorische Anforderungen der EU bedingte Testrahmen eingeführt, kommen auf die Finanzunternehmen möglicherweise höhere Kosten und Doppelarbeit zu. Daher wären Erleichterungen, Synchronisierung und EU-weite Zusammenarbeit ratsam.

Frage 28 Unterliegt Ihre Organisation derzeit Anforderungen in den Bereichen IKT und Sicherheitsprüfung?

- (●) Ja
- ( ) Nein
- ( ) Weiß ich nicht/keine Meinung/nicht relevant

Frage 28.1 Haben Sie Probleme mit sich überschneidenden oder abweichenden Pflichten?

- (●) Ja
- ( ) Nein
- ( ) Weiß ich nicht/keine Meinung/nicht relevant

Frage 28.2 Führen Sie in den Bereichen IKT und Sicherheit freiwillige Tests durch?

- (●) Ja
- ( ) Nein
- ( ) Weiß ich nicht/keine Meinung/nicht relevant

Frage 28.3 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 28 (und gegebenenfalls auf die entsprechenden Unterfragen):

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

In Deutschland sind Testanforderungen bereits in den Vorgaben der nationalen Aufsicht (MaRisk und BAIT iVm gängigen Standards z.B. ISO-Standard 2700x) enthalten. Sowohl technisch als auch fachlich-prozessuales Testing ist bereits ausreichend umfasst.
Unternehmen mit Standorten in mehreren Rechtsordnungssystemen sind häufig sich überschneidenden Anforderungen zu IKT- und Sicherheitstests von verschiedenen Behörden ausgesetzt, die auf das gleiche

Ziel ausgerichtet sind und massiv Ressourcen binden. Deshalb käme die Harmonisierung der Anforderungen für IKT- und Sicherheitstests sowohl den Unternehmen als auch den Behörden zugute.

Frage 29 Sollte von allen Finanzunternehmen verlangt werden, dass sie ihre IKT-Systeme und -Werkzeuge grundlegenden Tests bzw. Bewertungen unterziehen? Was könnten diese Tests bzw. Bewertungen umfassen?

	Ja	Nein	Weiß ich nicht/ keine Meinung/ nicht relevant
Lückenanalysen?	◉	○	○
Konformitätsprüfungen?	◉	○	○
Anfälligkeitsprüfungen?	◉	○	○
Prüfungen der physikalischen Sicherheit?	◉	○	○
Überprüfungen des Quellcodes?	○	○	◉

Frage 29.1 Gibt es weitere Elemente, die alle Finanzunternehmen zwingend in ihre grundlegenden Tests bzw. Bewertungen aufnehmen sollten? Bitte geben Sie an, welche und erläutern Sie Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 29.2 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 29:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Ein wirksames und für alle Finanzdienstleistungsunternehmen geltendes IKT- und Sicherheitsrisikomanagement-Rahmenwerk erfordert einen flexiblen, risikobasierten Ansatz, der sich an die sich schnell entwickelnden Risiken des Finanzsektors anpassen kann.
Finanzinstitute sollten geeignete Maßnahmen (Analysen, Assessments und Tests der Informationssicherheit) durchführen, um die effektive Identifizierung von Schwachstellen in ihren IKT-Systemen und IKT-Diensten zu gewährleisten. Derartige Maßnahmen werden bereits heute im Rahmen von

aufsichtlichen Prüfungen vorausgesetzt. Konkreten Methoden sollten nicht vorgeben werden. Die Auswahl aus den oben genannten Elementen ist jeweils abhängig von der Kritikalität und den Gegebenheiten vorzunehmen (Bsp.: Source Code Review für bezogene Software nicht möglich).

Frage 30 Sollten Finanzunternehmen für die Zwecke weitergehender Tests (z. B. Threat-Led-Penetration-Tests, TLPT) auf der Grundlage einer Kombination zum Beispiel der nachfolgenden Kriterien auf EU-Ebene oder von den zuständigen Behörden als „signifikant“ eingestuft werden?

	Ja	Nein	Weiß ich nicht/ keine Meinung/ nicht relevant
Proportionalitätsbezogene Faktoren (d. h. Größe, Art, Profil, Geschäftsmodell)	◉	○	○
Faktoren im Zusammenhang mit der Auswirkung (Kritikalität der erbrachten Dienste)	◉	○	○
Bedenken hinsichtlich der Finanzstabilität (systemische Bedeutung für die EU)	◉	○	○

Frage 30.1 Gibt es weitere geeignete qualitative oder quantitative Kriterien und Schwellen? Bitte geben Sie an, welche und erläutern Sie Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 30.2 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 30:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

TLPTs sind ein guter Baustein für einen effektiven Cybersecurity-Schutz und abhängig von der Kritikalität/ Signifikanz zu befürworten, insbesondere für Systeme, die für die Versorgungssicherheit der Bevölkerung

bzw. Finanzstabilität notwendig sind. Die Teilnahme an speziellen Red Teaming Tests (z.B. gemäß TIBER EU Rahmenwerk) unter Beteiligung von Aufsichtsbehörden sollte freiwillig erfolgen. Bei den Tests sollten vor allem die IT-Systeme und deren Betreiber (z.B. zentrale IT-Dienstleister) im Fokus stehen.

Frage 31 Sollte bei weitergehenden Tests (z. B. Threat-Led-Penetration-Tests) Folgendes zutreffen?

	Ja	Nein	Weiß ich nicht/ keine Meinung/ nicht relevant
Sollten alle Funktionen weitergehenden Tests unterzogen werden?	○	◉	○
Sollte der Schwerpunkt bei weitergehenden Tests auf Live-Produktionssystemen liegen?	○	○	◉
Sollten Finanzunternehmen zur Behandlung der Frage der Konzentration von Fachwissen im Falle von Testexperten eigene (interne) Experten einsetzen, die in Bezug auf die getesteten Funktionen operativ unabhängig sind?	◉	○	○
Sollten die Personen, die die Tests vornehmen, auf der Grundlage anerkannter internationaler Normen zertifiziert sein?	◉	○	○
Sollten außerhalb der Union vorgenommene Tests als gleichwertig anerkannt werden, sofern sie auf der Grundlage derselben Parameter durchgeführt (und somit für die Zwecke der EU-Regulierung als gültig angesehen) werden?	◉	○	○
Sollte es für die gesamte Union einen einheitlichen Testrahmen geben? Wäre TIBER-EU ein gutes Modell?	◉	○	○
Sollten die Europäischen Aufsichtsbehörden direkt an der Entwicklung eines harmonisierten Testrahmens beteiligt werden (z. B. indem sie Leitlinien herausgeben oder die Koordinierung sicherstellen)? Können Ihrer Ansicht nach andere EU-Gremien, etwa die Europäische Zentralbank bzw. der einheitliche Aufsichtsmechanismus, die Agentur der Europäischen Union für Cybersicherheit oder der Europäische Ausschuss für Systemrisiken, eine Rolle spielen?	○	○	◉
Sollten weitergehende Tests (z. B. Threat-Led-Penetration-Tests) in größerem Umfang vorgeschrieben werden?	○	◉	○

Frage 31.2 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 31:

höchstens 5000 Zeichen

einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Threat-Led-Penetration-Tests erfolgen mit dem Fokus, die Verwundbarkeit kritischer Systeme zu testen. Bei den Tests sollten jedoch die Auswirkungen auf die Sicherheit des Unternehmens und das Potenzial für Störungen berücksichtigt werden. In dieser Hinsicht müssen Tests auf Live-Produktionssystemen immer so ausgestaltet werden, dass sichergestellt ist, dass diese keine negativen Auswirkungen auf den Produktionsbetrieb haben bzw. das Bankgeschäft gefährden und keine Haftungsrisiken nach sich ziehen können. Eine valide Option ist, die Tests auf speziellen Testumgebungen eines Unternehmens vorzunehmen, die die Systeme der Produktion widerspiegeln. Das Testen aller Funktionen würde sich auch nicht als vorteilhaft erweisen, insbesondere nicht für Firmen, die eine gemeinsame Infrastruktur und einen konsistenten Kontrollrahmen haben; dies würde sich nur als doppeltes Vorgehen erweisen und die Kosten und die Testdauer unnötig erhöhen.
Eine mittelbare Risikokonzentration bei Red Teaming Dienstleistern sollte vermieden werden. Eine Zertifizierung hilft bei der Auswahl von externen Testern. Ein Testat sollte nicht zwingende Voraussetzung für die Beauftragung eines TLPT sein. Ebenso sollte die Verwendung der eigenen Red-Team-Ressourcen eines Unternehmens unterstützt werden, da dies dazu beitragen würde, Konzentrationsprobleme von Testexperten zu lösen und auch die Risikoexposition durch externe Tests zu verringern.
Ein harmonisierter EU-Testrahmen würde sowohl den Unternehmen als auch den Aufsichtsbehörden in ähnlicher Weise Vorteile bringen. TIBER-EU bzw. dessen nationale Ausgestaltung ist ein mögliches Modell für TLPTs. Bestehende Rahmen sollten in Betracht gezogen werden, um die gegenseitige Anerkennung solcher Tests voranzutreiben - nicht nur innerhalb der EU, sondern auch mit Nicht-EU-Peers, wo ähnliche Rahmen in Entwicklung oder bereits vorhanden sind, z.B. CBEST im Vereinigten Königreich. Im Einzelnen können aber auch weniger umfangreiche TLPTs bzw. Tests ohne Beteiligung der nationalen Behörden zur Erhöhung der Cybersicherheit beitragen.
TLPTs sollten auf freiwilliger Basis erfolgen. Eine detaillierte Sammlung von Schwachstellen sowie der etwaigen Maßnahmenpläne bei der Aufsicht oder bei Dritten erachten wir als nicht zielführend, da sich hierdurch das Risiko erhöht, dass Unberechtigte die Schwachstellen nutzen könnten (Risikokonzentration). Deshalb befürworten wir den Status Quo - ein europäisches Rahmenwerk als Orientierungsrahmen - darüberhinausgehende Leitlinien sind nicht erforderlich. Prinzipienorientiert sind Anforderungen bereits in den EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken enthalten.

Frage 32 In welchem Zeitabstand sollten diese Tests in Anbetracht ihrer zeitlichen und ressourcenmäßigen Auswirkungen am besten durchgeführt werden?

- ○ Halbjährlich
- ○ Jährlich
- ◉ Einmal alle drei Jahre
- ○ Sonstiges

Frage 32.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antwort auf Frage 32:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Die erweiterten Tests sollten eigenverantwortlich von signifikanten Instituten in das Gesamttestkonzept geplant und gesteuert werden (keine Vorgabe eines festen zeitlichen Rhythmus). Die Testhäufigkeit sollte

die praktischen Schritte berücksichtigen, die erforderlich sind, um den Nutzen der Testergebnisse zu maximieren und die Cyber-Resilienz-Fähigkeiten eines Unternehmens zu verbessern. Erweiterte Tests im Abstand von ca. drei Jahren würden einem Unternehmen genügend Zeit geben, um die Ergebnisse zu planen, zu testen, zu analysieren, Abhilfemaßnahmen zu planen und umzusetzen, bevor ein neuer Testzyklus beginnt.

Frage 33 Die Aktualisierungen, die Finanzunternehmen auf der Grundlage der Ergebnisse der Betriebsstabilitätsprüfung vornehmen, können als Katalysator für mehr Cyberresilienz wirken und so zur allgemeinen Finanzstabilität beitragen. Welche der folgenden Elemente könnten aufsichtsrechtliche Auswirkungen haben?

	Ja	Nein	Weiß ich nicht/ keine Meinung/ nicht relevant
Grundlegende Tests bzw. Bewertungsinstrumente (siehe Frage 29)	◉	○	○
Weitergehende Tests (z. B. Threat-Led-Penetration-Tests)	◉	○	○

Frage 33.1 Gibt es weitere Elemente, die aufsichtsrechtliche Auswirkungen haben könnten? Bitte geben Sie an, welche und erläutern Sie Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 33.2 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 33:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Es ist darauf zu achten, dass die verschiedenen Vorgehensweisen zur Wirksamkeitskontrolle der Sicherheitsmaßnahmen in einem ausgewogenen Verhältnis zum Einsatz kommen. Eine kontinuierliche Überwachung sowie regelmäßige (kostengünstigere) Maßnahmen sind zwingend notwendig, da sich Angriffsmuster kontinuierlich ändern und neue Sicherheitslücken in am Markt gekaufter Hardware- und Software auftreten. Die erweiterten Testmethoden z.B. TLPTs bilden für im Informationssicherheitsreifegrad fortgeschrittene Institute einen zusätzlichen Erkenntnisgewinn zum Stand der cyber resilience (good practise).

2.4. Minderung des Risikos von Drittschäden: Beaufsichtigung von Drittanbietern (einschließlich Auslagerung)

Finanzunternehmen greifen für die Auslagerung eines großen Teils ihrer Tätigkeiten auf externe IKT-Dienstleister zurück. Dies bringt zwar erhebliche Chancen mit sich, kann aber auch neue Risiken für Finanzunternehmen bergen und insbesondere zur Verlagerung bestehender Betriebs-, IKT-, Sicherheits-, Governance- und Reputationsrisiken auf externe Technologieanbieter führen. Darüber hinaus kann es zu Rechts- und Compliance-Problemen kommen, um nur einige zu nennen, die ihren Ursprung bei der Drittpartei haben oder sich aus IKT- und Sicherheitslücken innerhalb der Drittpartei ergeben können.

Der Rechtsrahmen sollte eine Reihe allgemeiner Grundsätze enthalten, die den verschiedenen Finanzinstituten bei der Gestaltung und Verwaltung vertraglicher Vereinbarungen mit Drittanbietern als Orientierung dienen und zudem einen besseren Überblick über die von Dritten ausgehenden Risiken und die nachfolgenden Auslagerungsketten ermöglichen.

Die weit verbreitete Nutzung von IKT-Drittanbietern kann zudem zu Konzentrationsrisiken bei der Verfügbarkeit von IKT-Drittanbietern, ihrer Substituierbarkeit und der Übertragbarkeit von Daten zwischen ihnen führen. Dies kann wiederum die Finanzstabilität beeinträchtigen. Einige IKT-Drittanbieter sind weltweit tätig, sodass Konzentrationsrisiken - zusammen mit anderen Risiken wie der Lokalisierung von Daten - weiter zunehmen. Dies gilt umso mehr im gegenwärtigen Kontext der regulatorischen Fragmentierung.

Die Europäischen Aufsichtsbehörden empfehlen die Einrichtung eines geeigneten Rahmens für die Beaufsichtigung von Dritten, um der Notwendigkeit einer besseren Überwachung der von IKT-Drittanbietern ausgehenden Risiken gerecht zu werden. Dabei sollte(n) Kriterien zur Identifizierung der kritischen Natur von IKT-Drittanbietern festgelegt, der Umfang der Aktivitäten, die in den Geltungsbereich dieses Rahmens fallen, definiert und die für die Aufsicht zuständige Behörde benannt werden.

Frage 34 Welche Kategorien von IKT-Drittanbietern nutzt Ihre Organisation am meisten? Soweit Sie es für erforderlich erachten, machen Sie bitte nähere Angaben.

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Deutscher Bankenmarkt:
Cloud-Dienstleister, Full-Service-Dienstleister, Software - und Hardware-Lieferanten, Telekommunikationsanbieter
Hinweis: In Deutschland haben in den Finanzgruppen organisierte Banken und Sparkassen Entwicklung und den Betrieb der IT zu großen Teilen an zentrale IT-Dienstleister der jeweiligen Finanzgruppe ausgelagert, der durch die Banken gesteuert wird. Es handelt sich hierbei nicht um klassische Drittdiensteanbieter, vielmehr besteht eine gelebte und funktionierende Arbeitsteilung von Beginn des IT-Zeitalters an. Diese Dienstleister sind direkt bzw. indirekt im Besitz der Banken und Sparkassen, so dass die Banken ihre Anforderungen geltend machen können.

Frage 35 Waren Sie während der Vertragsverhandlungen zwischen Ihrer Organisation und IKT-Drittanbietern mit Schwierigkeiten konfrontiert, insbesondere im Hinblick auf die Festlegung von Modalitäten, die die Anforderungen der Aufsichts- bzw. Regulierungsbehörden bezüglich der Auslagerung widerspiegeln?

- (•) Ja
- ( ) Nein
- ( ) Weiß ich nicht/keine Meinung/nicht relevant

Frage 35.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 35 und geben Sie an, welche spezifischen Anforderungen bezüglich der Auslagerung nur schwer im Vertrag bzw. in den Verträgen berücksichtigt werden konnten:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

IKT-Drittdiensteanbieter, einschließlich Anbieter von Cloud-Diensten, verfügen häufig bereits über Vertragsklauseln, die auf spezifische regulatorische Anforderungen der Branche eingehen. Sie sind grundsätzlich bereit, mit Finanzdienstleistungsunternehmen Klauseln zu erarbeiten, um spezifische interne oder regulatorische Anforderungen zu erfüllen (z. B. die Einhaltung der Compliance-Anforderungen der Unternehmen).
Vor allem im Bereich der großen Public Cloud-Dienstleister sind vertragliche Vereinbarungen in Teilen herausfordernd: Vereinbarung von Prüfrechten, Vereinbarung bzw. die Transparenz zu Sicherheitsvorgaben und die Kontrolle der Umsetzung sowie Exit-Strategien bei SaaS-Produkten. So gibt es beispielsweisen noch keine / wenige Standards um KI-Inhalte wie die Gewichtung eines neuronalen Netzes von einem Anbieter zu einem anderen zu migrieren.

Frage 36 Welche Anforderungen bezüglich der Auslagerung eignen sich im Rahmen der Arbeit der Kommission an Standardvertragsklauseln für Cloud-Vereinbarungen mit Unternehmen der Finanzbranche am besten für eine Standardisierung in freiwilligen Vertragsklauseln zwischen Finanzunternehmen und externen IKT-Dienstleistern (z. B. Cloud)? Soweit Sie es für erforderlich erachten, machen Sie bitte nähere Angaben.

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Über die neuen EBA-Leitlinien zur Auslagerung werden spezielle bankaufsichtliche Anforderungen an Auslagerungen hinreichend definiert, die auch das Cloud-Outsourcing umfassen. Diese Entwicklungen haben den Banken und IKT-Drittanbietern Klarheit über die vertraglichen Anforderungen und Verpflichtungen des Auslagerungsmanagements geschaffen.
Eine weitere Harmonisierung zur Standardisierung von Vertragsklauseln zwischen Finanzdienstleistungsunternehmen und IKT-Drittdiensteanbietern sollte nicht zu zusätzlichen obligatorischen Anforderungen führen und weiterhin einen risiko- und prinzipienbasierten Ansatz ermöglichen.
Technisch wird der Standard ISO/IEC 27017:2015 als angemessen betrachtet, da dieser ergänzend zu den ISO/IEC 27002- und ISO/IEC 27001-Normen Leitlinien zu Aspekten der Informationssicherheit beim Cloud

Computing enthält. Für jeden Bereich der übergeordneten Norm ISO/IEC 27001 werden mögliche Besonderheiten der Cloud-Sicherheit explizit dargelegt. Durch diese Methodik können Sicherheitsvorgaben schneller identifiziert und in das Sicherheitsmanagementsystem integriert werden.

Frage 37 Was halten Sie von der möglichen Einführung eines Aufsichtsrahmens für IKT-Drittanbieter?

	Ja	Nein	Weiß ich nicht/ keine Meinung/ nicht relevant
Sollte ein Aufsichtsrahmen geschaffen werden?	◉	○	○
Sollte sich dieser auf kritische IKT-Drittanbieter konzentrieren?	◉	○	○
Sollte die „Kritikalität“ auf einer Reihe von sowohl qualitativen als auch quantitativen Schwellenwerten beruhen (z. B. Konzentration, Anzahl der Kunden, Größe, Vernetzung, Substituierbarkeit, Komplexität usw.)?	◉	○	○
Sollte die Verhältnismäßigkeit bei der Identifizierung kritischer IKT-Drittanbieter eine Rolle spielen?	◉	○	○
Sollten andere damit zusammenhängende Aspekte (z. B. Datenportabilität, Exit-Strategien und damit verbundene Marktpraktiken, faire Vertragspraktiken, Umweltleistung usw.) in den Aufsichtsrahmen aufgenommen werden?	◉	○	○
Sollten die für die aufsichtsrechtliche oder organisatorische Überwachung von Finanzunternehmen zuständigen Behörden auf europäischer und nationaler Ebene die Aufsicht übernehmen?	◉	○	○
Sollte ein Kooperationsmechanismus eingerichtet werden (z. B. innerhalb von Aufsichtskollegien, wobei eine nationale zuständige Behörde bei der Beaufsichtigung eines relevanten IKT-Dienstleisters eines ihrer Aufsicht unterstehenden Unternehmens die Leitung übernimmt - siehe z. B. das in der neuen Bankenrichtlinie vorgesehene Modell)?	○	○	◉
Sollten die Überwachungsinstrumente auf unverbindliche Instrumente beschränkt werden (z. B. Empfehlungen, grenzüberschreitende Zusammenarbeit durch gemeinsame Inspektionen und Informationsaustausch, Überprüfungen vor Ort usw.)?	○	◉	○
Sollte die Überwachung auch verbindliche Instrumente (wie Sanktionen oder andere Durchsetzungsmaßnahmen) umfassen?	◉	○	○

Frage 37.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 37:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Für die Einführung von Rahmenbedingungen zur Überwachung von IKT-Drittanbietern ist eine gründliche Bewertung erforderlich, um Einschränkungen bei der Nutzung von Drittdiensten und damit verbundene Auswirkungen auf die Innovationsfähigkeit, den Wettbewerb und das Geschäftsmodell der Banken zu vermeiden.
Die Diskussion über dieses Thema und mögliche europäische Anforderungen sollte aufgrund der Vernetzung der Finanzdienstleistungen und der Größe der IKT-Anbieter, wie z.B. Cloud-Anbieter, global koordiniert werden.
Sofern eine direkte Beaufsichtigung von Drittdiensteanbietern beabsichtigt wird, sollten gleiche Regeln für alle Marktteilnehmer gelten. Es sollte ebenfalls darauf geachtet werden, dass entsprechende Regelungen mit den bereits vorhandenen Vorgaben harmonisiert bzw. koordiniert werden, so dass kein separates Rahmenwerk allein für IKT-Drittdiensteanbieter geschaffen wird. Ein eventuelles Rahmenwerk sollte dabei auch der Beschaffenheit eines global agierenden Finanzsystems Rechnung tragen.

Frage 38 Welche Lösungen halten Sie für die geeignetsten und wirksamsten, um dem Konzentrationsrisiko bei externen IKT-Dienstleistern zu begegnen?

	Ja	Nein	Weiß ich nicht/ keine Meinung/ nicht relevant
Diversifizierungsstrategien, einschließlich eines potenziellen obligatorischen oder freiwilligen Rotationsmechanismus mit entsprechenden Regeln zur Gewährleistung der Übertragbarkeit (z. B. Prüfungsmodell)	○	◉	○
Obligatorischer Mehranbieter-Ansatz	○	◉	○
Sollten vom Gesetzgeber oder den Aufsichtsbehörden Grenzen gesetzt werden, um die übermäßige Exposition eines Finanzinstituts gegenüber einem oder mehreren IKT-Drittanbietern zu bekämpfen?	○	◉	○

Frage 38.1 Gibt es andere Lösungen, die Ihrer Meinung nach am geeignetsten und wirksamsten sind, um dem Konzentrationsrisiko bei externen IKT-Dienstleistern zu begegnen? Bitte geben Sie an, welche und erläutern Sie Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 38.2 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 38:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Effektives Outsourcing und IKT- und Sicherheitsrisikomanagement erfordert einen flexiblen, risikobasierten Ansatz, der sich an die sich schnell entwickelnde Landschaft des Finanzsektors anpassen kann. Es sollte vermieden werden, verbindliche Methoden zum Umgang mit Konzentrationsrisiken bei IKT-Drittanbietern (z. B. Mehranbieteransatz, Expositionsgrenzen, Rotationsmechanismen) vorzuschreiben, da dies die Fähigkeit eines Unternehmens, seine Widerstandsfähigkeit kontinuierlich zu verbessern und sich an neue Geschäftsmodelle und Technologien anzupassen, behindern kann.
Wir unterstützen die Förderung des Wettbewerbs und die Erhöhung der Portabilität und Interoperabilität zwischen IKT-Drittanbietern. Jedoch lösen unseres Erachtens die vorgeschlagenen Ansätze das Konzentrationsrisiko nicht - die Konzentration von Dienstleistungen würde weiterhin in einer kleinen Anzahl von Unternehmen verdichtet sein. Die Nutzung mehrerer Provider erhöht die Komplexität der IT für die Bank sogar weiter (Komplexitätsrisiko steigt).
Eine Exit-/Wechsel-Strategie sollte grundsätzlich im Sinne der Diversifikation berücksichtigt werden. Die Cloud-Anbieter sollten dazu angehalten werden, dies durch offene Schnittstellen und Datenformate sowie durch den Nachweis der Migrationsfähigkeit zu unterstützen.

2.5. Weitere Bereiche, in denen EU-Maßnahmen erforderlich sein können

---

Informationsaustausch: In diesem Teil geht es um den Austausch von Informationen zwischen verschiedenen Finanzunternehmen, bei dem es sich nicht um Meldungen (der Finanzunternehmen an die zuständigen Behörden) oder die Zusammenarbeit (zwischen den zuständigen Behörden) handelt.

Der Informationsaustausch trägt dazu bei, Cyberangriffen und der Verbreitung von IKT-Bedrohungen vorzubeugen. Der Informationsaustausch zwischen Finanzunternehmen - etwa der Austausch über Taktiken, Techniken und Verfahren sowie Kompromissindikatoren - leistet einen Beitrag zur Gewährleistung eines sicheren und zuverlässigen IKT-Umfelds, das für das Funktionieren des integrierten und vernetzten Finanzsektors von entscheidender Bedeutung ist.

Frage 39 Stimmen Sie zu, dass die EU eine Rolle bei der Unterstützung und Förderung des freiwilligen Austauschs solcher Informationen zwischen Finanzinstitutionen spielen sollte?

- (●) Ja
- ( ) Nein
- ( ) Weiß ich nicht/keine Meinung/nicht relevant

Frage 39.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 39:

höchstens 5000 Zeichen

einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Cyberangriffe sind in vergangenen Jahren lokal unterschiedlich ausgeprägt aufgetreten. Erfolgreiche Methoden wurden zumindest zu einem späteren Zeitpunkt auch in anderen Ländern versucht.
Der Finanzsektor verfügt bereits über ein angemessenes Instrumentarium und Mechanismen für den Informationsaustausch (siehe Frage 40). Deshalb besteht kein Bedarf, zusätzliche verbindliche Anforderungen zu schaffen, die auf den Informationsaustausch ausgerichtet sind und die den qualitativen Input dieser vertrauenswürdigen Netzwerke einschränken können. Vielmehr könnte die Kommission die Marktteilnehmer dafür sensibilisieren, die derzeit bestehenden Mechanismen und Instrumente für den Informationsaustausch zu nutzen.
Erkenntnisse der Behörden über besondere oder gehäufte Angriffsmuster aus den bestehenden Meldungen der Finanzinstitute sollten darüberhinaus für ein Lagebild und in anonymisierter Form als Ausgangspunkt für einen Informationsaustausch im Finanzsektor genutzt werden.

Frage 40 Ist Ihre Organisation derzeit Teil solcher Vereinbarungen über den Austausch von Informationen?

- (•) Ja
- ( ) Nein
- ( ) Weiß ich nicht/keine Meinung/nicht relevant

Wenn Sie Frage 40 mit „Ja“ beantwortet haben, erläutern Sie bitte, wie diese Vereinbarungen organisiert sind und mit welchen Finanzpartnern Sie diese Informationen austauschen. Bitte geben Sie die Art der ausgetauschten Informationen und die Häufigkeit des Austauschs an:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Ein Austausch zwischen Finanzinstituten und Dienstleistern erfolgt auf nationaler und internationaler Ebene. Dieser ist in der Regel informell organisiert und basiert auf der vertrauensvollen und kooperativen Zusammenarbeit der Beteiligten. Wesentliche Voraussetzung für den Informationsaustausch ist ein gegenseitiges Kennen und eine hieraus resultierende Vertrauensbasis.
Es gibt aktuell bereits eine Vielzahl an Austauschplattformen. Diese definieren sich zum einen thematisch oder sind regional organisiert. Einen großen Stellenwert hat der Austausch zu Angriffsszenarien auf kritische Infrastrukturen. Ein Austausch zu Themen des Cybercrimes besteht zudem zwischen Banken und Behörden in Deutschland z.B. mit dem Bundeskriminalamt sowie diversen Landeskriminalämtern (Kriminalpolizei des Bundes und der Länder in Deutschland) sowie dem Bundesamt für Sicherheit in der Informationstechnik (Nationale Sicherheitsbehörde). Als Schnittstelle werden direkte Kontakte und SPOC-Strukturen genutzt. Darüber hinaus sind einzelne Institute in weiteren Organisationen zum Information Sharing z.B. G4C (Deutschland) bzw. FS-ISAC (International) aktiv vertreten.

Frage 40.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 40 (und gegebenenfalls auf die entsprechende Unterfrage):

höchstens 5000 Zeichen

einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Dem freiwilligen Austausch von Informationen kommt eine hohe Bedeutung sowohl für die Prävention als auch für die Eindämmung von Cyber-Angriffen zu.

Frage 41 Birgt der Austausch von Informationen über Cyberbedrohungen und -vorfälle mit gleichgestellten Finanzinstituten Ihrer Meinung nach besondere Herausforderungen?

- (●) Ja
- ( ) Nein
- ( ) Weiß ich nicht/keine Meinung/nicht relevant

Wenn Sie Frage 41 mit „Ja“ beantwortet haben, erläutern Sie bitte anhand konkreter Beispiele die Herausforderungen und deren Gründe:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Kritisch ist zu sehen, dass das Wissen zu Angriffen und Angriffsmustern zunehmend nicht kostenfrei geteilt, sondern kommerziell verwertet wird und damit nur denen zur Verfügung steht, die für diese Informationen bezahlen.
Eine weitere Herausforderung stellt die Sanitarisierung der ausgetauschten Informationen dar. Einerseits müssen die Informationen soweit anonymisiert werden, dass kein Rückschluss auf das jeweils meldende Haus möglich ist. Andererseits birgt eine zu starke Sanitarisierung das Risiko, dass die geteilten Informationen für die Empfänger wertlos werden. Für den Austausch zwischen Beteiligten der Finanzindustrie bedarf es eines Vertrauensankers, der die Vertraulichkeit der ausgetauschten Informationen sicherstellt.
Es steigt andererseits auch die Gefahr geflutet zu werden, je mehr Informationen ausgetauscht werden.

Frage 41.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 41 (und gegebenenfalls auf die entsprechende Unterfrage):

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 42 Sind Sie der Meinung, dass ein verstärkter Informationsaustausch innerhalb des EU-Rechtsraums erforderlich ist?

- (●) Ja
- ( ) Nein
- ( ) Weiß ich nicht/keine Meinung/nicht relevant

Frage 42.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 42 und legen Sie dar, welche Art von Informationen ausgetauscht werden sollten und warum ihr Austausch zweckdienlich ist:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Ein EU-weiter Austausch macht dann Sinn, wenn die Angriffe auch in anderen Ländern zu finden sind. Grundsätzlich verfügt der Finanzsektor auch über ausreichende Instrumentarien und Mechanismen für den EU-weiten Informationsaustausch. Um die Möglichkeiten für einen grenzüberschreitenden freiwilligen Austausch zu verbessern, wäre es hilfreich, Inkonsistenzen und Unsicherheiten zu adressieren, die Beschränkungen für den Austausch von Bedrohungsinformationen bedeuten können.

Förderung von Cyberversicherungen und anderen Regelungen zur Risikoübertragung: In einem zunehmend digitalisierten Finanzsektor, der mit zahlreichen Cybervorfällen konfrontiert ist, müssen die Finanzinstitute und ihre Aufsichtsbehörden ein besseres Verständnis für die Rolle entwickeln, die der Versicherungsschutz gegenüber Cyberrisiken spielen kann. Sowohl die Nachfrage- als auch die Angebotsseite des europäischen Marktes für Cyberversicherungen und andere Risikoübertragungsinstrumente sollten einer weiteren Analyse unterzogen werden.

Frage 43 Verfügt Ihre Organisation derzeit über eine Art Cyberversicherung oder Risikoübertragungspolitik?

- ( ) Ja
- ( ) Nein
- (●) Weiß ich nicht/keine Meinung/nicht relevant

Frage 43.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 43 (und gegebenenfalls auf die entsprechende Unterfrage):

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Cyber-Versicherungen stellen eine Möglichkeit des Risikotransfers dar. Die Entscheidung für eine Absicherung ist institutsspezifisch auf Basis von Risikoassessments unter Berücksichtigung des Proportionalitätsprinzips und des Risikoappetits zu entscheiden. Die Fragen 43 - 46 beziehen sich insofern auf Anforderungen einzelner Institute. Eine übergreifende Beantwortung dieser Fragen durch die Deutsche Kreditwirtschaft als Interessensvertretung der fünf deutschen kreditwirtschaftlichen Spitzenverbände ist nicht möglich.

Frage 44 Welche Arten von Cyberversicherungs- oder Risikoübertragungsprodukten würde Ihre Organisation kaufen bzw. für welche Arten von Cyberversicherungs- oder Risikoübertragungsprodukten sehen Sie einen Bedarf? Soweit Sie es für erforderlich halten, machen Sie bitte nähere Angaben dazu, ob diese Produkte eher Eigenschäden oder Drittschäden oder eine Kombination aus beidem abdecken sollten:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 45 Was sind Ihrer Meinung nach die Herausforderungen bei der Entwicklung eines europäischen Cyberversicherungs- bzw. Risikoübertragungsmarktes, falls es solche gibt?

	Ja	Nein	Weiß ich nicht/ keine Meinung/ nicht relevant
Fehlen einer gemeinsamen Taxonomie für Cybervorfälle	○	○	○
Mangel an verfügbaren Daten über Cybervorfälle	○	○	○
Mangelndes Bewusstsein über die Bedeutung von Cyber-/IKT-Sicherheit	○	○	○
Schwierigkeiten bei der Preiskalkulation oder der Einschätzung der Risiken	○	○	○
Rechtsunsicherheit hinsichtlich der Vertragsbedingungen und der Abdeckung	○	○	○

Frage 45.1 Gibt es Ihrer Meinung nach weitere Herausforderungen bei der Entwicklung eines europäischen Cyberversicherungs- bzw.

R i s i k o ü b e r t r a g u n g s m a r k t e s ?
Bitte geben Sie an, welche und erläutern Sie Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 45.2 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 45 und legen Sie so genau wie möglich dar, wie diese Probleme oder Mängel angegangen werden könnten:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Frage 46 Sollte die EU irgendeine Art von Unterstützung für die Entwicklung von europäischen oder nationalen Initiativen zur Förderung von Entwicklungen in diesem Bereich leisten?

- Ja
- Nein
- Weiß ich nicht/keine Meinung/nicht relevant

Frage 46.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 46 (und gegebenenfalls auf die entsprechenden Unterfragen):

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

2.6. Interaktion mit der Richtlinie zur Netz- und Informationssicherheit

Die Richtlinie zur Netz- und Informationssicherheit ist das erste horizontale Binnenmarktinstrument, das auf die Verbesserung der Widerstandsfähigkeit der EU gegen Cybersicherheitsrisiken in verschiedenen kritischen Sektoren (siehe Anhang II der Richtlinie) durch die Gewährleistung eines Mindestmaßes an Harmonisierung abzielt.

Im Bereich der Finanzdienstleistungen fallen Unternehmen aus drei Sektoren in den Anwendungsbereich der Richtlinie: Kreditinstitute, Betreiber von Handelsplätzen und zentrale Gegenparteien. Unternehmen aus anderen Finanzdienstleistungssektoren (z. B. Versicherungs- und Rückversicherungsunternehmen, Transaktionsregister, Zentralverwahrer, Dienstleistungsunternehmen im Bereich Datenmeldung, Vermögensverwalter, Wertpapierfirmen, Kreditratingagenturen usw.) sind von dem Anwendungsbereich der Richtlinie ausgeschlossen. Die einschlägigen IKT- und Sicherheitsrisikoanforderungen dieser Unternehmen werden weiterhin in anderen spezifischen Rechtsvorschriften geregelt.

Die Lex-specialis-Klausel der Richtlinie zur Netz- und Informationssicherheit ermöglicht die Anwendung sektorspezifischer EU-Rechtsakte, wenn diese Anforderungen in Bezug auf die Sicherheit von Netz- und Informationssystemen oder die Meldung von Sicherheitsvorfällen enthalten, die den in der Richtlinie enthaltenen Anforderungen gleichwertig sind.[11]

Was Unternehmen anbelangt, die den in Anhang II der Richtlinie zur Netz- und Informationssicherheit genannten kritischen Sektoren angehören, so haben die Mitgesetzgeber den Mitgliedstaaten bei der Festlegung, welche speziellen Unternehmen in diesen kritischen Sektoren in den Anwendungsbereich der Richtlinie fallen sollten, einen breiten Ermessensspielraum eingeräumt. Insbesondere sind die Mitgliedstaaten verpflichtet, die Identifizierung von „Betreibern wesentlicher Dienste“ auf der Grundlage von drei in der Richtlinie festgelegten Kriterien vorzunehmen.

[11] Artikel 1 Absatz 7 der Richtlinie: „… und sind diese Anforderungen in ihrer Wirkung den in dieser Richtlinie enthaltenen Pflichten mindestens gleichwertig, so gelten die einschlägigen Bestimmungen jenes sektorspezifischen Rechtsakts der Union.“

Frage 47 Fällt Ihre Organisation in den Anwendungsbereich der Richtlinie zur Netz- und Informationssicherheit, so wie sie in Ihrem Mitgliedstaat umgesetzt wird (d. h. gilt Ihre Organisation als Betreiber wesentlicher Dienste)?

- ○ Ja
- ◉ Nein
- ○ Weiß ich nicht/keine Meinung/nicht relevant

Frage 47.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 47 (und gegebenenfalls auf die entsprechende Unterfrage):

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Ausgewählte Mitgliedsinstitute der Verbände fallen unter das IT-Sicherheitsgesetz (nationale Umsetzung der NIS-Directive). Hierin wird für diese Institute eine Umsetzung der IT-Sicherheit nach dem „Stand der Technik “ vorgeschrieben. Zudem wird durch das IT-Sicherheitsgesetz die Meldung von erheblichen IT-Sicherheitsvorfällen an das Bundesamt für Sicherheit in der Informationstechnik geregelt.

Frage 48 Wie würden Sie die Auswirkungen der Richtlinie zur Netz- und Informationssicherheit für Ihre spezifische Finanzorganisation bewerten? Wie würden Sie die Auswirkungen der Richtlinie auf Ihren Finanzsektor unter Berücksichtigung der drei spezifischen Finanzsektoren, die in den Anwendungsbereich der Richtlinie zur Netz- und Informationssicherheit fallen (Kreditinstitute, Handelsplätze und zentrale Clearingstellen), der Benennung von Betreibern wesentlicher Dienste und der Lex-specialis-Klausel bewerten?
Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Den Anforderungen der NIS-Richtlinie wird im Bankensektor bereits durch die bankaufsichtlichen Anforderungen Rechnung getragen. Die nationalen Regelungen des IT-Sicherheitsgesetzes führen somit zu zusätzlichen Verpflichtungen durch das Reporting an die nationale Sicherheitsbehörde und zu doppelter Meldung von Betriebs- und Sicherheitsvorfällen an nationale Sicherheitsbehörde und Bankenaufsicht mit unterschiedlichen Meldeschemen. Im Falle eines Sicherheitsvorfalls müssen mehrere Meldungen mit z. T. unterschiedlichen Inhalten an unterschiedliche Empfänger abgegeben werden.
Insgesamt sollte die Kommission ihre Bemühungen nicht auf die Gewährleistung einer detaillierten Konsistenz bei der nationalen Umsetzung konzentrieren, sondern vielmehr sicherstellen, dass die Wirksamkeit der Regelungen erreicht wird und dass es kein schwaches Glied in der Kette gibt.

Frage 49 Gelten für Sie Anforderungen, die im Vergleich zu den in der Richtlinie zur Netz- und Informationssicherheit festgelegten Anforderungen spezifischer sind? Wenn ja, handelt es sich dabei um Anforderungen gemäß den EU-Vorschriften für Finanzdienstleistungen oder Anforderungen gemäß nationalem Recht?
Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Ausführungen:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Weitere konkretisierende Anforderungen an das Informationssicherheitsmanagement/-risikomanagement ergeben sich aus den Vorschriften der nationalen Bankenaufsichtsbehörde Bundesanstalt für Finanzdienstleistungen (BaFin) “Bankaufsichtliche Anforderungen an die IT (BAIT)”.

Sonderfrage: Zur Auswahl der folgenden an Sie zu stellenden Fragen geben Sie bitte an, ob es sich bei Ihrer Organisation um Folgendes handelt:

- ○ in einem Mitgliedstaat ansässiges Finanzinstitut, für den als zuständige Behörde im Sinne der Richtlinie zur Netz- und Informationssicherheit eine nationale Behörde benannt wurde, bei der es sich nicht um eine Finanzaufsichtsbehörde handelt
- ○ Finanzaufsichtsbehörde, zuständige Behörde im Sinne der Richtlinie zur Netz- und Informationssicherheit, zentrale Anlaufstelle
- ◉ weder noch

Die Fragen 50 und 51 sind speziell an in einem Mitgliedstaat ansässige Finanzinstitute gerichtet, der als zuständige Behörde im Sinne der Richtlinie zur Netz- und Informationssicherheit eine nationale Behörde benannt hat, bei der es sich nicht um eine Finanzaufsichtsbehörde handelt.

Die Fragen 52 bis 56 richten sich spezifisch an Finanzaufsichtsbehörden, benannte zuständige Behörden im Sinne der Richtlinie zur Netz- und Informationssicherheit und zentrale Anlaufstellen gerichtet.

3. Mögliche Auswirkungen

Die Initiative dürfte einen Beitrag zur Schaffung eines sichereren digitalen Umfelds für den Betrieb und die Nutzung komplexer IKT-Werkzeuge und -Prozesse leisten, die die Grundlage für die Erbringung von Finanzdienstleistungen bilden. Es wird davon ausgegangen, dass eine solche Erhöhung der Betriebsstabilität der digitalen Systeme der Finanzinstitute insgesamt (die IKT- und Sicherheitsrisiken umfasst) nicht nur positive Auswirkungen auf die allgemeine Finanzstabilität haben, sondern auch zu einem höheren Verbraucherschutzniveau führen und innovative datengesteuerte Geschäftsmodelle im Finanzbereich ermöglichen würde.

Frage 57 Bitte geben nach Möglichkeit und auf der Grundlage der in den vorstehenden Abschnitten zu den verschiedenen Bausteinen angegebenen Informationen an, welche möglichen Folgen und Auswirkungen (d. h. wirtschaftliche, soziale, unternehmerische Auswirkungen oder Folgen bzw. Auswirkungen im Hinblick auf die Geschäftsentwicklung usw.) Sie sowohl kurz- als auch langfristig vorhersehen können. Bitte erläutern Sie Ihre Ausführungen und machen Sie genaue Angaben:

höchstens 5000 Zeichen

einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Europaweit einheitliche IT-Sicherheitsstandards und eine Harmonisierung der Aufsichtspraktiken unterstützen grundsätzlich die Anstrengungen zur Verbesserung der Sicherheit von Finanzsystemen, wenn diese risikoadäquat für alle Marktteilnehmer ausgestaltet werden. Ein Rahmenwerk, dass nicht risikoorientiert ausgestaltet ist und kleinteilige, detaillierte Vorgaben macht, würde zu einer weiteren Erhöhung der Ausgaben für Compliance-Themen, weiteren Einschränkungen bei unternehmerischen Entscheidungen sowie dem Rückgang der Rentabilität des Finanzsektors und Verlust der Bankendiversität führen.
Einheitliche Vorgaben sollten sich sinnvoll in ein einheitliches Aufsichtskonzept gegenüber Finanzdienstleistern und Banken einfügen und ein Rahmenwerk bilden, in welchem die Akteure Handlungsspielraum haben. Die Vorgaben und die Prüfungshandlungen sollten sich an internationalen Standards und Best Practices orientieren, um eine einheitliche Prüfungspraxis zu gewährleisten.
Insgesamt bietet das Vorhaben Chancen für die verschiedenen Akteure in der EU, wenn die Kommission ihre Anstrengungen auf Vorgaben konzentriert, die mit den bereits bestehenden globalen und regionalen Prinzipien und Vorschriften in Bezug auf Cyber- und IKT-Risiken konsistent sind und sich nicht wiederholen, die prinzipienorientiert sind und auf Mindestanforderungen des Managements von Cyber- und IKT-Risiken im gesamten EU-Finanzdienstleistungssektor basieren.

Frage 58 Welche der in den vorstehenden Abschnitten zu den Bausteinen dargelegten spezifischen Maßnahmen würden den größten Nutzen und Wert für Ihre Organisation und Ihren Finanzsektor bringen?

Haben Sie zudem eine Abschätzung des Nutzens und der einmaligen und /oder wiederkehrenden Kosten dieser spezifischen Maßnahmen vorgenommen?
Bitte erläutern Sie Ihre Ausführungen und machen Sie genaue Angaben:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Von folgenden Maßnahmen würde der Finanzsektor am meisten profitieren:
• Harmonisierung der regulatorischen Vorgaben und Herleitung auf Basis von internationalen Standards und Best Practices gleichermaßen für alle Marktteilnehmer,
• Verringerung der regulatorischen Inkonsistenzen und Fragmentierung z.B. bei der Meldung von Sicherheitsvorfällen,
• Fokussierung auf eine effiziente und möglichst standardisierte Gestaltung des Regulierungsrahmens,
• Nutzung der internationalen Zusammenarbeit, wo immer möglich (z.B. gemeinsame Nutzung von TLPT-Testergebnissen),
• Förderung des Wettbewerbs im Bereich der Oligopole im Public Cloud Markt.

Frage 59 Welche dieser spezifischen Maßnahmen wären für Ihre Organisation völlig neu und würden möglicherweise weitere Schritte bzw. einen schrittweisen Ansatz bei ihrer Umsetzung erfordern?
Bitte erläutern Sie Ihre Ausführungen und machen Sie genaue Angaben:

höchstens 5000 Zeichen

einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Die Fragen 59 / 60 und 62 können nur unternehmensspezifisch beantwortet werden. Eine übergreifende Beantwortung dieser Fragen durch die Deutsche Kreditwirtschaft als Interessensvertretung der fünf deutschen kreditwirtschaftlichen Spitzenverbände ist nicht möglich.

Frage 60 Wo genau erwarten Sie, dass Ihr Unternehmen die größten Anstrengungen unternimmt, um zukünftigen verschärften Maßnahmen bezüglich des IKT-Risikomanagements und den erhöhten Sicherheitsvorkehrungen im digitalen Umfeld gerecht zu werden? Erwarten Sie zum Beispiel in Bezug auf Ihre derzeitige IKT-Sicherheitsbasis, dass ein Schwerpunkt darauf gelegt wird, mehr in die Modernisierung von Technologien zu investieren, eine Unternehmensdisziplin einzuführen, die Einhaltung neuer Bestimmungen wie etwa Testanforderungen zu gewährleisten usw.?
Bitte erläutern Sie Ihre Ausführungen und machen Sie genaue Angaben:

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

siehe Frage 59

Frage 61 Welche Verwaltungsformalitäten oder -anforderungen in Bezug auf IKT-Risiken sind heute aus wirtschaftlicher Sicht am aufwändigsten, personalintensivsten oder kostenineffizientesten? Wie sollte Ihrer Meinung nach damit umgegangen werden?
Bitte erläutern Sie Ihre Ausführungen und machen Sie genaue Angaben:

höchstens 5000 Zeichen

einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

Die Frequenz von Anfragen von verschiedenen Teilen der Aufsicht (Fragebögen) und die Häufigkeit von Onsite Inspections sowie die mangelnde Harmonisierung im Meldewesen zu Sicherheitsvorfällen.

Frage 62 Haben Sie eine Schätzung der Kosten (unmittelbaren Kosten und Folgekosten) vorgenommen, die Ihrem Unternehmen aufgrund von IKT-Vorfällen und insbesondere Cyberangriffen entstanden sind?

- Ja
- Nein
- Weiß ich nicht/keine Meinung/nicht relevant

Frage 62.1 Soweit Sie es für erforderlich erachten, erläutern Sie bitte Ihre Antworten auf Frage 62 (und gegebenenfalls auf die entsprechende Unterfrage):

höchstens 5000 Zeichen
einschließlich Leerzeichen und Zeilenumbrüchen, d. h. strenger als die Zeichenzählung bei MS Word.

siehe Frage 59

Weitere Angaben

Sollten Sie zusätzliche Informationen zur Verfügung stellen (z. B. ein Positionspapier, Bericht) oder ein bestimmtes Thema ansprechen wollen, das in der Konsultation nicht abgedeckt wurde, können Sie Ihr zusätzliches (Ihre zusätzlichen) Dokument(e) hier hochladen:

Die maximale Dateigröße beträgt 1 MB.
Sie können mehrere Dateien hochladen.

Useful links

Mehr zum Transparenzregister (http://ec.europa.eu/transparencyregister/public/homePage.do?locale=en)

Einzelheiten der Konsultation (https://ec.europa.eu/info/publications/finance-consultations-2019-financial-services digital-resilience_en)

Spezielle Datenschutzerklrung (https://ec.europa.eu/info/law/better-regulation/specific-privacy-statement_en)

Konsultationsdokument (https://ec.europa.eu/info/files/2019-financial-services-digital-resilience-consultation-document_en)

Contact

fisma-digital-operational-resilience@ec.europa.eu