Rådet for
Den Europæiske Union

Bruxelles, den 24. september 2020
(OR. en)

11051/20

Interinstitutionel sag:
2020/0266(COD)

EF 228
ECOFIN 846
TELECOM 159
CYBER 168
IA 61
CODEC 871

FORSLAG

fra:	Jordi AYET PUIGARNAU, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	24. september 2020
til:	Jeppe TRANHOLM-MIKKELSEN, generalsekretær for Rådet for Den Europæiske Union
Komm. dok. nr.:	COM(2020) 595 final
Vedr.:	Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 og (EU) nr. 909/2014

Hermed følger til delegationerne dokument COM(2020) 595 final.

Bilag: COM(2020) 595 final

EUROPA-
KOMMISSIONEN

Bruxelles, den 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 og (EU) nr. 909/2014

(EØS-relevant tekst)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

- Begrundelse for og målene med forslaget

Dette forslag er en del af pakken om digital finans, som er en pakke af foranstaltninger, som yderligere skal frigive og understøtte det potentiale, der ligger i digital finans med hensyn til innovation og konkurrence, samtidig med at de risici, der følger heraf, reduceres. Det er i overensstemmelse med Kommissionens prioriteter om at gøre Europa klar til den digitale tidsalder og opbygge en fremtidssikret økonomi, der tjener alle. Pakken om digital finans indeholder en ny strategi for digital finans for EU's finansielle sektor[1], som har til formål at sikre, at EU tager den digitale revolution til sig og fremmer den med innovative europæiske virksomheder i front, idet forbrugere og virksomheder får adgang til fordelene ved digital finans. Ud over dette forslag indeholder pakken også et forslag til forordning om markeder for kryptoaktiver[2], et forslag til forordning om en pilotordning for markedsinfrastrukturer baseret på distributed ledger-teknologi (DLT)[3] og et forslag til direktiv, der skal præcisere eller ændre visse relaterede EU-regler om finansielle tjenesteydelser[4].Digitalisering og operationel modstandsdygtighed i den finansielle sektor er to sider af samme sag. Digitale teknologier eller informations- og kommunikationsteknologier (IKT) giver anledning til såvel muligheder som risici. Der skal være god forståelse for og styring af dem, navnlig i perioder med stresspåvirkning.

Politiske beslutningstagere og tilsynsmyndigheder retter derfor i stigende grad fokus mod risici, som skyldes afhængighed af IKT. De har navnlig forsøgt at øge virksomheders modstandsdygtighed ved at fastsætte standarder og ved at koordinere det regulerings- eller tilsynsmæssige arbejde. Dette arbejde er blevet udført på både internationalt og europæisk plan samt både på tværs af industrisektorer og for en række specifikke sektorer, herunder sektoren for finansielle tjenesteydelser.

IKT-risici udgør ikke desto mindre fortsat en udfordring for den operationelle modstandsdygtighed, kapaciteten og stabiliteten i EU's finansielle system. Den reform, der fulgte efter den finansielle krise i 2008, øgede primært den finansielle modstandsdygtighed[5] i EU's finansielle sektor, idet den kun indirekte imødegik IKT-risici på visse områder som led i foranstaltningerne til at afhjælpe operationelle risici mere bredt.

---

1 Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Den Europæiske Centralbank, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om en strategi for digital finans for EU (COM(2020) 591 af 23.9.2020).

2 Forslag til Europa-Parlamentets og Rådets forordning om markeder for kryptoaktiver og om ændring af direktiv (EU) 2019/1937 (COM(2020) 593).

3 Forslag til Europa-Parlamentets og Rådets forordning om en pilotordning for markedsinfrastrukturer baseret på distributed ledger-teknologi (COM(2020) 594).

4 Forslag til Europa-Parlamentets og Rådets direktiv om ændring af direktiv 2006/43/EF, 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 (COM(2020) 596).

5 De forskellige foranstaltninger, der blev vedtaget, havde grundlæggende til formål at øge finansielle enheders kapitalressourcer og likviditet samt at reducere markeds- og kreditrisici.

Mens der med ændringerne af EU-lovgivningen om finansielle tjenesteydelser efter krisen blev indført et fælles regelsæt, som regulerer store dele af de finansielle risici, der er forbundet med finansielle tjenesteydelser, tog disse ikke fuldt ud højde for digital operationel modstandsdygtighed. De foranstaltninger, der er truffet med hensyn til sidstnævnte, var karakteriseret ved en række egenskaber, der begrænsede deres effektivitet. For eksempel blev de ofte udarbejdet som minimumsharmoniseringsdirektiver eller principbaserede forordninger, som giver betydelig fleksibilitet til divergerende tilgange i hele det indre marked. Derudover har der kun været begrænset eller ufuldstændigt fokus på IKT-risici i forbindelse med dækningen af operationelle risici. Endelig varierer disse foranstaltninger på tværs af den sektorspecifikke lovgivning om finansielle tjenesteydelser. Med andre ord svarede tiltagene på EU-plan ikke fuldt ud til det, som europæiske finansielle enheder havde brug for med henblik på styring af operationelle risici på en måde, der sikrer modstandsdygtighed, en indsats over for og genopretning efter virkningerne af IKT-hændelser. De gav heller ikke finansielle tilsynsmyndigheder de bedst egnede værktøjer til at opfylde deres mandater til at forebygge finansiel instabilitet, som skyldes, at sådanne IKT-risici reelt opstår.

Manglen på detaljerede og udførlige regler om digital operationel modstandsdygtighed på EU-plan har ført til udbredelse af nationale reguleringsinitiativer (f.eks. afprøvning af digital operationel modstandsdygtighed) og tilsynsmetoder (f.eks. håndtering af afhængighed af tredjepartsudbydere af IKT). Tiltag på nationalt plan har imidlertid kun begrænset indvirkning på grund af IKT-risicis grænseoverskridende karakter. De ukoordinerede nationale initiativer har desuden resulteret i overlapninger, manglende konsekvens, duplikering af krav, høje administrations- og overholdelsesomkostninger — navnlig for grænseoverskridende finansielle enheder — eller i, at IKT-risici ikke detekteres og dermed ikke imødegås. Denne situation medfører fragmentering på det indre marked, underminerer stabiliteten og integriteten i EU's finansielle sektor og sætter forbruger- og investorbeskyttelsen på spil.

Det er derfor nødvendigt at indføre en detaljeret og udførlig ramme for digital operationel modstandsdygtighed for EU's finansielle enheder. Denne ramme vil uddybe den dimension, der vedrører digital risikostyring i det fælles regelsæt. Den vil navnlig styrke og strømline finansielle enheders udførelse af IKT-risikostyring, indføre en grundig afprøvning af IKT-systemer, øge tilsynsmyndigheders kendskab til cyberrisici og de IKT-relaterede hændelser, som finansielle enheder udsættes for, samt tillægge finansielle tilsynsmyndigheder beføjelser til at føre tilsyn med risici, som skyldes finansielle enheders afhængighed af tredjepartsudbydere af IKT-tjenester. Forslaget vil skabe en konsekvent mekanisme til indberetning af hændelser, som vil bidrage til at mindske den administrative byrde for finansielle enheder og øge den tilsynsmæssige effektivitet.

- Sammenhæng med de gældende regler på samme område.

Dette forslag indgår som led i et bredere igangværende arbejde på europæisk og internationalt plan for at styrke cybersikkerheden i forbindelse med finansielle tjenesteydelser og imødegå bredere operationelle risici[6].

Det kommer også som reaktion på den fælles tekniske rådgivning[7] fra 2019 fra de europæiske tilsynsmyndigheder (ESA'er), hvori der opfordres til en mere konsekvent tilgang til

[6] Baselkomitéen for Banktilsyn, *Cyber-resilience: Range of practices*, december 2018 and *Principles for sound management of operational risk (PSMOR)*, oktober 2014.

imødegåelse af IKT-risici inden for finans og det anbefales, at Kommissionen på en forholdsmæssigt afpasset måde styrker den digitale operationelle modstandsdygtighed i sektoren for finansielle tjenesteydelser gennem et sektorspecifikt EU-initiativ. ESA'ernes rådgivning var en reaktion på Kommissionen fintechhandlingsplan fra 2018[8].

- Sammenhæng med Unionens politik på andre områder

Som Kommissionens formand, Ursula von der Leyen, erklærede i sine politiske retningslinjer[9] og som beskrevet i meddelelsen "Europas digitale fremtid i støbeskeen"[10] er det afgørende for Europa at høste alle fordelene ved den digitale tidsalder og styrke sin industri- og innovationskapacitet inden for sikre og etiske grænser. I den europæiske strategi for data[11] fastsættes der fire søjler — databeskyttelse, grundlæggende rettigheder, sikkerhed og cybersikkerhed — som væsentlige forudsætninger for et samfund, der styrkes ved brugen af data. I den seneste tid har Europa-Parlamentet været beskæftiget med en betænkning om digital finans, som bl.a. opfordrer til en fælles tilgang til cyberrobusthed i den finansielle sektor[12].En lovramme, der øger den digitale operationelle modstandsdygtighed i EU's finansielle enheder, er i overensstemmelse med disse politikmål. Forslaget vil også understøtte politikker, der sigter mod genopretning efter covid-19, da dette vil sikre, at øget afhængighed af digital finans går hånd i hånd med operationel modstandsdygtighed.

Initiativet vil bevare de fordele, der er forbundet med det horisontale ramme om cybersikkerhed (f.eks. direktivet om cybersikkerhed, NIS-direktivet), ved fortsat at lade den finansielle sektor indgå i dens anvendelsesområde. Den finansielle sektor vil fortsat være tæt forbundet med NIS-samarbejdsorganet, og finansielle tilsynsmyndigheder vil få mulighed for at udveksle relevante oplysninger inden for det eksisterende NIS-økosystem. Initiativet vil være i overensstemmelse med direktivet om europæisk kritisk infrastruktur, som i øjeblikket revideres for at styrke beskyttelsen af og modstandsdygtigheden i kritiske infrastrukturer mod ikke-cyberrelaterede trusler. Endelig er dette forslag i fuld overensstemmelse med strategien for EU's sikkerhedsunion[13], som opfordrer til et initiativ om digital operationel modstandsdygtighed i den finansielle sektor, da den i høj grad er afhængig af IKT-tjenester og sårbar over for cyberangreb.

---

7 Fælles rådgivning fra de europæiske tilsynsmyndigheder til Europa-Kommissionen om behovet for lovgivningsmæssige forbedringer vedrørende kravene til IKT-risikostyring i EU's finansielle sektor , JC 2019 26 (2019).

8 Europa-Kommissionen, *Fintechhandlingsplan* (COM(2018) 109 final).

9 Kommissionens formand, Ursula von der Leyen, *Politiske retningslinjer for den næste Europa-Kommission*, 2019-2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

10 Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget: *Europas digitale fremtid i støbeskeen* (COM(2020) 67 final).

11 Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget: *En europæisk strategi for data* (COM(2020) 66 final).

12 "Betænkning med anbefalinger til Kommissionen om digital finans: nye risici forbundet med kryptoaktiver — regulerings- og tilsynsmæssige udfordringer på området finansielle tjenester, institutioner og markeder (2020/2034(INL))", https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en.

13 Meddelelse fra Kommissionen til Europa-Parlamentet, Det Europæiske Råd, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om strategien for EU's sikkerhedsunion (COM(2020) 605 final).

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

- Retsgrundlag

Forslaget til forordning bygger på artikel 114 i TEUF.

Den fjerner hindringer for og forbedrer etableringen af det indre marked for finansielle tjenesteydelser og dets funktionsmåde ved at harmonisere de regler, der gælder på området for IKT-risikostyring, indberetning, afprøvning og IKT-tredjepartsrisici. Nuværende forskelle på dette område, både på lovgivnings- og reguleringsmæssigt plan samt på nationalt plan og EU-plan, udgør hindringer på det indre marked for finansielle tjenesteydelser, fordi finansielle enheder, der indgår i grænseoverskridende aktiviteter, står over for forskellige, hvis ikke ligefrem overlappende, reguleringsmæssige krav eller tilsynsmæssige forventninger, som potentielt kan hindre dem i at udøve deres frie etableringsret og ret til fri udveksling af tjenesteydelser. Forskellige regler forvrider ligeledes konkurrencen mellem den samme type finansielle enheder i forskellige medlemsstater. På områder, hvor ikke findes harmonisering, delvist eller i begrænset omfang, kan udviklingen af divergerende nationale regler eller tilgange, som enten allerede er trådt i kraft eller er ved at blive vedtaget og gennemført på nationalt plan, udgøre hindringer for udøvelsen af frihedsrettighederne på det indre marked for finansielle tjenesteydelser. Dette er navnlig tilfældet for rammerne for afprøvning af digital operationel modstandsdygtighed og tilsynet med kritiske tredjepartsudøvere af IKT-tjenester.

Da forslaget har virkninger for flere af Europa-Parlamentets og Rådets direktiver, som er vedtaget på grundlag af artikel 53, stk. 1, i TEUF, vedtages der på samme tid et forslag til direktiv for at afspejle de nødvendige ændringer af nævnte direktiver.

- Nærhedsprincippet

Den høje grad af indbyrdes forbundethed på tværs af finansielle tjenesteydelser, finansielle enheders betydelige grænseoverskridende aktiviteter og den udbredte afhængighed af tredjepartsudbydere af IKT-tjenester i den finansielle sektor som helhed nødvendiggør aktivering af en stor digital operationel modstandsdygtighed som et spørgsmål af fælles interesse for at bevare sunde finansielle EU-markeder. Forskelle, som skyldes uensartede eller delvise ordninger, overlapninger eller flere krav, der gælder for de samme finansielle enheder, som har aktiviteter på tværs af grænserne eller er indehavere af adskillige tilladelser[14] i hele det indre marked, kan udelukkende tackles effektivt på EU-plan.

Dette forslag harmoniserer den digitale operationelle komponent i en dybt integreret sektor med indbyrdes forbundethed, som allerede nyder godt af et fælles regelsæt og tilsyn på det fleste andre centrale områder. For spørgsmål såsom indberetning af IKT-relaterede hændelser kan kun harmoniserede EU-regler mindske den administrative byrde og de finansielle omkostninger, der er forbundet med indberetning af den IKT-relaterede hændelse til forskellige EU-myndigheder og nationale myndigheder. Der er også brug for EU-tiltag, som kan lette den gensidige anerkendelse af resultaterne af avanceret afprøvning af digital operationel modstandsdygtighed for enheder, der har aktiviteter på tværs af grænserne, og

[14] En og samme finansielle enhed kan have tilladelser til henholdsvis at udøve bankvirksomhed, udøve virksomhed som investeringsselskab og betalingsinstitut, som hver er meddelt af en forskellig tilsynsmyndighed i en eller adskillige medlemsstater.

som i mangel af EU-regler er eller kan blive omfattet af forskellige rammer i forskellige medlemsstater. Kun tiltag på EU-plan kan afhjælpe forskellene i de afprøvningsmetoder, som medlemsstaterne har indført. Tiltag på EU-plan er også nødvendige for at afhjælpe manglen på passende tilsynsbeføjelser med henblik på overvågning af risici, der skyldes tredjepartsudbydere af IKT-tjenester, herunder koncentrationsrisici og afsmitningsrisici i EU's finansielle sektor.

- Proportionalitetsprincippet

De foreslåede bestemmelser går ikke videre, end hvad der er nødvendigt for at nå forslagets mål. Det omfatter kun aspekter, som medlemsstaterne ikke kan varetage på egen hånd, og hvor den administrative byrde og omkostningerne står i rimeligt forhold til de specifikke og generelle mål, der skal nås.

Med hensyn til anvendelsesområde og intensitet er proportionalitetsprincippet udformet gennem anvendelse af kvalitative og kvantitative vurderingskriterier. Disse kriterier har til formål at sikre, at de nye regler, samtidig med at de dækker alle finansielle enheder, også er skræddersyet til risici og behov i forhold til enhedernes specifikke karakteristika for så vidt angår deres størrelse og virksomhedsprofiler. Proportionalitetsprincippet indgår også i reglerne om IKT-risikostyring, afprøvning af digital modstandsdygtighed, indberetning af større IKT-relaterede hændelser og tilsyn med kritiske tredjepartsudbydere af IKT-tjenester.

- Valg af retsakt

De foranstaltninger, som er nødvendige for at regulere IKT-risikostyring, indberetning af IKT-relaterede hændelser, afprøvning af og tilsyn med kritiske tredjepartsudbydere af IKT-tjenester, skal være indeholdt i en og samme forordning for at sikre, at de detaljerede krav kan anvendes effektivt og direkte på en ensartet måde, uden at det berører proportionalitetsprincippet og de specifikke regler, der fastsættes i denne forordning. Sammenhæng i måden, hvorpå digitale operationelle risici håndteres, bidrager til at øge tilliden til det finansielle system og bevarer dets stabilitet. Da anvendelsen af en forordning bidrager til at mindske reguleringsmæssig kompleksitet, fremme tilsynsmæssig konvergens og øge retssikkerheden, bidrager denne forordning også til at begrænse finansielle enheders overholdelsesomkostninger, navnlig for dem, der har aktiviteter på tværs af grænserne, hvilket igen kan bidrage til at fjerne konkurrenceforvridninger.

Ved denne forordning ryddes også lovgivningsmæssige forskelle og uensartede nationale regulerings- eller tilsynsmæssige tilgange til IKT-risici af vejen, og dermed fjernes hindringer for det indre marked for finansielle tjenesteydelser, navnlig for en problemfri udøvelse af den frie etableringsret og af retten til fri udveksling af tjenesteydelser for finansielle enheder med grænseoverskridende tilstedeværelse.

Endelig er det fælles regelsæt primært blevet udarbejdet ved hjælp af forordninger, og ajourføring heraf med komponenten vedrørende digital operationel modstandsdygtighed bør ske efter samme valg af retligt instrument.

3. RESULTATER AF EFTERFØLGENDE EVALUERINGER, HØRINGER AF INTERESSEREDE PARTER OG KONSEKVENSANALYSER

- Efterfølgende evalueringer/kvalitetskontrol af gældende lovgivning

Hidtil har ingen EU-lovgivning om finansielle tjenesteydelser sat fokus på operationel modstandsdygtighed, og ingen har på fyldestgørende vis imødegået risici, som skyldes digitalisering, ikke engang de regler, som mere overordnet vedrører den operationelle risikodimension med IKT-risici som delkomponent. Hidtidige EU-tiltag har bidraget til at imødekomme behov og afhjælpe problemer, der opstod i kølvandet på den finansielle krise i 2008: Kreditinstitutterne havde ikke et tilstrækkeligt kapitalgrundlag, de finansielle markeder var ikke tilstrækkeligt integrerede, og harmoniseringen var indtil da blevet holdt på et minimum. IKT-risici blev ikke betragtet som en prioritet på daværende tidspunkt, og som følge heraf har lovrammerne for de forskellige finansielle delsektorer udviklet sig på en ukoordineret måde. Unionen har gennem sine tiltag alligevel nået sine mål om at sikre finansiel stabilitet og om fastlægge et fælles set harmoniserede tilsynsregler og regler for markedsadfærd, som finder anvendelse på finansielle enheder i hele EU. Det synes udfordrende at foretage en eksplicit evaluering, da de faktorer, der førhen gav anledning til lovgivningsmæssige tiltag på EU-plan, ikke muliggjorde specifikke eller udførlige regler for at håndtere den udbredte anvendelse af digitale teknologier og deraf følgende risici inden for finans. En implicit evaluering og deraf følgende lovgivningsmæssige ændringer er afspejlet i hver af denne forordnings søjler.

- Høringer af interesserede parter

Kommissionen har hørt interesserede parter under hele processen med udarbejdelsen af dette forslag, navnlig

i) gennemførte Kommissionen en særlig åben offentlig høring (19. december 2019 – 19. marts 2020)[15]

ii) hørte Kommissionen offentligheden om en indledende konsekvensanalyse (19. december 2019 – 16. januar 2020)[16]

iii) hørte Kommissionens tjenestegrene eksperter fra medlemsstaterne i Ekspertgruppen om Bankvirksomhed, Betalinger og Forsikring (EGBPI) to gange (den 18. maj 2020 og den 16. juli 2020)[17]

iv) afholdt Kommissionens tjenestegrene et særligt webinar om digital operationel modstandsdygtighed, som indgik i rækken af arrangementer vedrørende Digital Finance Outreach 2020 (den 19. maj 2020).

Formålet med den offentlige høring var at orientere Kommissionen om udarbejdelsen af en potentiel EU-ramme for digital operationel modstandsdygtighed i forbindelse med finansielle tjenesteydelser. Besvarelserne viste, at der var bred tilslutning til at indføre en særlig ramme med tiltag med fokus på de fire områder, der indgik i høringen, samtidig med at det understreges, at det er nødvendigt at sikre proportionalitet og omhyggeligt at tage højde for og redegøre for samspillet med de horisontale regler i NIS-direktivet. Kommissionen modtog to

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

besvarelser vedrørende den indledende konsekvensanalyse, hvor respondenterne behandlede specifikke aspekter forbundet med deres respektive aktivitetsområder.

På mødet i EGBPI, der fandt sted den 18. maj 2020, udtrykte medlemsstaterne bred tilslutning til en styrkelse af digital operationel modstandsdygtighed i den finansielle sektor gennem de påtænkte tiltag, der lægger sig op ad de fire elementer, som Kommissionen har beskrevet. Medlemsstaterne understregede også behovet for klar samordning af de nye regler med reglerne om operationelle risici (i EU-lovgivningen om finansielle tjenesteydelser) og med de horisontale regler om cybersikkerhed (i henhold til NIS-direktivet). På det andet møde understregede nogle medlemsstater behovet for at sikre proportionalitet og tage hensyn til den særlige situation for små virksomheder og datterselskaber i større koncerner samt behovet for at sikre et stærkt mandat for nationale kompetente myndigheder, der er involveret i tilsyn.

Forslaget bygger også på og integrerer feedback fra møder med interessenter og EU-myndigheder og -institutioner. Interessenter, herunder tredjepartsudbydere af IKT-tjenester, har generelt givet opbakning hertil. En analyse af den modtagne feedback viser et ønske om at bevare proportionaliteten og at følge en princip- og risikobaseret tilgang i forbindelse med udformningen af regler. På institutionelt plan kom de primære input fra Det Europæiske Udvalg for Systemiske Risici (ESRB), ESA'erne, Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) og Den Europæiske Centralbank (ECB) samt fra medlemsstaternes kompetente myndigheder.

- Indhentning og brug af ekspertbistand

Ved udarbejdelsen af dette forslag har Kommissionen taget udgangspunkt i kvalitativ og kvantitativ evidens fra anerkendte kilder, herunder de to sæt fælles teknisk bistand fra ESA'erne. Dette er blevet suppleret med fortrolige input og offentligt tilgængelige rapporter fra tilsynsmyndigheder, internationale standardiseringsorganer og førende forskningsinstitutter samt kvantitative og kvalitative input fra identificerede interessenter i hele den globale finansielle sektor.

- Konsekvensanalyse

Dette forslag ledsages af en konsekvensanalyse[18], som blev indgivet til Udvalget for Forskriftskontrol den 29. april 2020 og godkendt den 29. maj 2020. Udvalget anbefalede forbedringer på nogle områder med henblik på i) at give flere oplysninger om, hvordan der vil blive sikret proportionalitet, ii) bedre at fremhæve, i hvilket omfang den foretrukne løsning er forskellig fra ESA'ernes fælles tekniske rådgivning, og hvorfor den pågældende løsning er den mest optimale, og iii) yderligere at fremhæve, hvordan forslaget indgår i samspil med eksisterende EU-lovgivning, herunder med regler, der er ved at blive revideret. Konsekvensanalysen blev tilpasset for at behandle disse punkter samt for at tage hensyn til de mere detaljerede bemærkninger fra Udvalget for Forskriftskontrol.

Kommissionen overvejede følgende række politikløsninger med henblik på at udvikle en ramme for digital operationel modstandsdygtighed:

[18] Arbejdsdokument fra Kommissionens tjenestegrene — Impact Assessment Report Accompanying the document Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (SWD(2020)198 af 24.9.2020).

- "Der træffes ingen foranstaltninger": Der vil fortsat blive fastsat regler om operationel modstandsdygtighed i henhold til det nuværende, divergerende sæt EU-bestemmelser om finansielle tjenesteydelser, delvist under NIS-direktivet, og i henhold til eksisterende eller fremtidige nationale ordninger.

- Løsning 1: Styrkelse af kapitalbuffere: Der vil blive indført supplerende kapitalbuffere for at øge finansielle enheders evne til at dække tab, der kan opstå som følge af mangel på digital operationel modstandsdygtighed.

- Løsning 2: Indførelse af en retsakt om digital operationel modstandsdygtighed i forbindelse med finansielle tjenesteydelser: Muliggørelse af en udførlig ramme på EU-plan med sammenhængende regler, som imødekommer alle regulerede finansielle enheders behov for digital operationel modstandsdygtighed, og som fastlægger en tilsynsramme for kritiske tredjepartsudbydere af IKT-tjenester.

- Løsning 3: En retsakt om digital operationel modstandsdygtighed i forbindelse med finansielle tjenesteydelser kombineret med et centraliseret tilsyn med kritiske tredjepartsudbydere af IKT-tjenester: Foruden en retsakt om digital operationel modstandsdygtighed (løsning 2), vi der blive oprettet en ny myndighed, der skal føre tilsyn med leveringen af tjenester fra tredjepartsudbydere af IKT-tjenester.

Den anden løsning blev valgt, fordi den opfylder flest af de tilsigtede mål på en måde, der er effektiv, virkningsfuld og sammenhængende med andre EU-politikker. De fleste interessenter foretrækker også denne løsning.

Den valgte løsning vil give anledning til både engangsomkostninger og tilbagevendende omkostninger[19]. Engangsomkostningerne skyldes primært investeringer i IT-systemer og er som sådan vanskelige at kvantificere, da virksomheders komplekse landskaber, og navnlig deres nedarvede IT-systemer, er i forskellig stand. Alligevel vil disse omkostninger sandsynligvis være begrænsede for større virksomheder, da de allerede har foretaget betydelige investeringer i IKT. Omkostningerne forventes også at være begrænsede for mindre virksomheder, da forholdsmæssigt afpassede foranstaltninger vil finde anvendelse på grund af deres lavere risiko.

Den valgte løsning vil have positive virkninger for SMV'er, der har aktiviteter i sektoren for finansielle tjenesteydelser, for så vidt angår den økonomiske, sociale og miljømæssige indvirkning. Forslaget vil skabe klarhed for SMV'er om de regler, som finder anvendelse, hvilket vil mindske overholdelsesomkostninger.

Den primære sociale indvirkning af den valgte politikløsning vil komme til udtryk blandt forbrugere og investorer. Højere niveauer af digital operationel modstandsdygtighed i EU's finansielle system vil mindske antallet af og de gennemsnitlige omkostninger forbundet med hændelser. Samfundet som helhed vil drage fordel af den øgede tillid til sektoren for finansielle tjenesteydelser.

Med hensyn til miljømæssig indvirkning vil den valgte politikløsning endelig tilskynde til øget anvendelse af den nyeste generation af IKT-infrastrukturer og -tjenester, som rent miljømæssigt forventes at blive mere bæredygtige.

[19] Ibid, s. 89-94.

- Målrettet regulering og forenkling

Afskaffelse af overlappende krav vedrørende indberetning af IKT-relaterede hændelser vil reducere den administrative byrde og mindske de dermed forbundne omkostninger. Derudover vil harmoniseret afprøvning af digital operationel modstandsdygtighed med gensidig anerkendelse i hele det indre marked mindske omkostningerne, navnlig for grænseoverskridende virksomheder, der ellers kunne blive underlagt flere test i flere medlemsstater[20].

- Grundlæggende rettigheder

EU har forpligtet sig at sikre til et højt niveau af beskyttelse af de grundlæggende rettigheder. Alle frivillige ordninger for informationsudveksling mellem finansielle enheder, som fremmes i nærværende forordning, vil blive gennemført i et pålideligt miljø under fuld overholdelse af EU's databeskyttelsesregler, navnlig Europa-Parlamentets og Rådets forordning (EU) 2016/679[21], og navnlig når det er nødvendigt at behandle personoplysninger med henblik på en legitim interesse, som forfølges af den dataansvarlige.

4. VIRKNINGER FOR BUDGETTET

Da ESA'erne i den nuværende forordning tildeles en vigtigere rolle i form af beføjelser, som de tillægges med henblik på at føre tilstrækkeligt tilsyn med kritiske tredjepartsudbydere af IKT-tjenester, vil forslaget med hensyn til virkninger for budgettet medføre tildeling af øgede ressourcer, navnlig for at fuldføre tilsynsmissioner (f.eks. inspektioner på stedet og online samt revisioner) og anvendelse af personale, der besidder specifik IKT-sikkerhedsekspertise.

Omfanget og fordelingen af disse omkostninger vil afhænge af omfanget af de nye tilsynsbeføjelser og de (præcise) opgaver, som ESA'erne skal varetage. Med hensyn til at stille nye personaleressourcer til rådighed vil EBS, ESMA og EIOPA i alt have brug for 18 fuldtidsansatte (FTÆ) — 6 FTÆ'er for hver myndighed — når forslagets forskellige bestemmelser tages i anvendelse (anslået til 15,71 mio. EUR for perioden 2022-2027). ESA'erne vil også pådrage sig yderligere IT-omkostninger, missionsudgifter til inspektioner på stedet og udgifter til oversættelse (anslået til 12 mio. EUR for perioden 2022-2027) samt andre administrationsudgifter (anslået til 2,48 mio. EUR for perioden 2022-2027). Derfor ligger de samlede anslåede omkostningsmæssige virkninger på omkring 30,19 mio. EUR for perioden 2022-2027.

Det bør ligeledes bemærkes, at mens det nødvendige antal ansatte (f.eks. nye medarbejdere og andre udgifter forbundet med de nye opgaver) med henblik på direkte tilsyn over tid vil afhænge af udviklingen i det antal kritiske tredjepartsudbydere af IKT-tjenester, der skal føres tilsyn med, og disses størrelse, vil de respektive udgifter blive fuldt ud finansieret af gebyrer, der opkræves hos de pågældende markedsdeltagere. Derfor forventes der ingen virkninger for EU's budgetbevillinger (med undtagelse af de yderligere medarbejdere), da disse omkostninger vil blive fuldt ud finansieret af gebyrer.

---

20 Ibid.

21 Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

Der gøres nærmere rede for dette forslags finansielle og budgetmæssige virkninger i finansieringsoversigten til forslaget.

5. ANDRE FORHOLD

- Planer for gennemførelsen og foranstaltninger til overvågning, evaluering og rapportering

Forslaget indeholder en generel plan for overvågning og evaluering af indvirkningen på de specifikke mål, som kræver, at Kommissionen foretager en revision tidligst tre år efter forordningens ikrafttræden og aflægger rapport til Europa-Parlamentet og Rådet om sine vigtigste konklusioner.

Denne revision skal foretages i overensstemmelse med Kommissionens retningslinjer for bedre regulering.

- Nærmere redegørelse for de enkelte bestemmelser i forslaget

Forslaget er opbygget omkring adskillige vigtige politikområder, som er centrale indbyrdes forbundne søjler, der ved fælles enighed er indarbejdet i europæiske og internationale vejledninger samt europæisk og international bedste praksis med det formål at styrke cyberrobustheden og den operationelle modstandsdygtighed i den finansielle sektor.

Forordningens anvendelsesområde og forholdsmæssigt afpasset anvendelse af de påkrævede foranstaltninger (artikel 2)

For at sikre sammenhæng med hensyn til de krav til IKT-risikostyring, som finder anvendelse på den finansielle sektor, dækker forordningen en række finansielle enheder, som er reguleret på EU-plan, navnlig kreditinstitutter, betalingsinstitutter, e-pengeinstitutter, investeringsselskaber, udbydere af kryptoaktivtjenester, centrale værdipapircentraler, centrale modparter, markedspladser, transaktionsregistre, forvaltere af alternative investeringsfonde og administrationsselskaber, udbydere af dataindberetningstjenester, forsikrings- og genforsikringsselskaber, forsikringsformidlere, genforsikringsformidlere, accessoriske forsikringsformidlere, arbejdsmarkedsrelaterede pensionskasser, kreditvurderingsbureauer, revisorer og revisionsfirmaer, administratorer af kritiske benchmarks og udbydere af crowdfundingtjenester.

En sådan dækning fremmer en homogen og sammenhængende anvendelse af alle de komponenter, der indgår i risikostyring på IKT-relaterede områder, samtidig med at den bevarer de lige vilkår blandt finansielle enheder med hensyn til deres lovgivningsmæssige forpligtelser vedrørende IKT-risici. På samme tid anerkendes det i forordningen, at der findes betydelige forskelle mellem finansielle enheder for så vidt angår størrelse, forretningsprofiler eller deres eksponering for digitale risici. Da større finansielle enheder har flere ressourcer, er det kun finansielle enheder, som ikke betragtes som mikrovirksomheder, der f.eks. skal indføre komplekse ledelsesordninger, særlige ledelsesfunktioner, foretage tilbundsgående vurderinger efter større ændringer af infrastrukturer for net- og informationssystemer, regelmæssigt foretage risikoanalyser af nedarvede IKT-systemer, udvide afprøvningen af driftsstabiliteten samt indsats- og genopretningsplaner for at tegne et billede af overgangsscenarier mellem deres primære IKT-infrastruktur og redundante faciliteter. Desuden er det kun finansielle enheder, der er identificeret som betydelige med henblik på

afprøvning af avanceret digital modstandsdygtighed, der vil skulle udføre trusselsbaserede penetrationstest.

Til trods for at denne dækning er bred, er den ikke udtømmende. Navnlig tages der i denne forordning hverken højde for systemoperatører, jf. definitionen i artikel 2, litra p), i direktiv 98/26/EF om endelig afregning i betalingssystemer og værdipapirafviklingssystemer (finalitydirektivet)[22], eller systemdeltagere, medmindre en sådan deltager selv er en finansiel enhed, der er reguleret på EU-plan, og dermed som sådan vil være dækket af denne forordning som selvstændig enhed (f.eks. kreditinstitut, investeringsselskab, CCP). Derudover falder EU's register for emissionskvoter, som drives i overensstemmelse med direktiv 2003/87/EF[23] i Europa-Kommissionens regi, også uden for anvendelsesområdet.

Ved sådanne udelukkelser fra finalitydirektivet tages der højde for behovet for en yderligere vurdering af retlige og politiske anliggender, der vedrører systemoperatører og -deltagere i henhold til finalitydirektivet, samtidig med at der tages behørigt hensyn til indvirkningen af de rammer, der på nuværende tidspunkt finder anvendelse på betalingssystemer[24], der drives af centralbanker. Da disse anliggender kan indebære aspekter, som fortsat er forskellige fra de spørgsmål, der er omfattet af denne forordning, vil Kommissionen fortsat vurdere nødvendigheden og indvirkningen af en yderligere udvidelse af denne forordnings anvendelsesområde til at omfatte IKT-infrastrukturer, som på nuværende tidspunkt ligger uden for dets anvendelsesområde.

Ledelsesrelaterede krav (artikel 4)

Denne forordning er udformet med henblik på en bedre tilpasning af finansielle enheders forretningsstrategier og gennemførelse af IKT-risikostyring. Til dette formål skal ledelsesorganet fortsat spille en afgørende, aktiv rolle i styringen af rammen for IKT-risikostyring og tilstræbe respekt for en streng cyberhygiejne. Ledelsesorganets fulde ansvar for styring af finansielle enheders IKT-risici vil være et overordnet princip, der skal udmøntes yderligere i en række specifikke krav såsom tildelingen af klare roller og ansvarsområder for alle IKT-relaterede funktioner, et fortsat engagement i kontrol med overvågningen af IKT-risikostyringen samt i hele spektret af godkendelses- og kontrolprocesser og en hensigtsmæssig tildeling af IKT-investeringer og -kurser.

Krav til IKT-risikostyring (artikel 5-14)

Digital operationel modstandsdygtighed bygger på et sæt centrale principper og krav vedrørende rammen for IKT-risikostyring i overensstemmelse med den fælles tekniske bistand fra ESA'erne. Disse krav, der tager udgangspunkt i relevante standarder, retningslinjer og henstillinger, der er fastlagt på internationalt og nationalt plan samt på sektorplan, drejer sig om specifikke funktioner inden for IKT-risikostyring (identifikation, beskyttelse og forebyggelse, detektion, indsats og genopretning, læring og udvikling samt kommunikation). For at holde trit med et cybertrusselsbillede i hastig udvikling pålægges det finansielle

---

22 Europa-Parlamentets og Rådets direktiv 98/26/EF af 19. maj 1998 om endelig afregning i betalingssystemer og værdipapirafviklingssystemer (EFT L 166 af 11.6.1998, s. 45).

23 Europa-Parlamentets og Rådets direktiv 2003/87/EF af 13. oktober 2003 om et system for handel med kvoter for drivhusgasemissioner i Unionen og om ændring af Rådets direktiv 96/61/EF (EUT L 275 af 25.10.2003, s. 32).

24 Navnlig Den Europæiske Centralbanks forordning (EU) nr. 795/2014 af 3. juli 2014 om overvågningskrav for systemisk vigtige betalingssystemer.

enheder at oprette og vedligeholde modstandsdygtige IKT-systemer og -værktøjer, der mindsker virkningerne af IKT-risici, løbende at identificere alle kilder til IKT-risici, at træffe beskyttelses- og forebyggelsesforanstaltninger, øjeblikkeligt at detektere anomale aktiviteter, at indføre målrettede og udførlige driftsstabilitetspolitikker samt katastrofe- og genopretningsplaner som en integreret del af politikken for operationel driftsstabilitet. Sidstnævnte komponenter er nødvendige med henblik på en hurtig genopretning efter IKT-relaterede hændelser, navnlig cyberangreb, ved at begrænse skaden og prioritere en sikker genoptagelse af aktiviteter. Forordningen selv indfører ikke en specifik standardisering, men bygger snarere på europæiske og internationalt anerkendte tekniske standarder eller bedste praksis i sektoren, for så vidt som de er i fuld overensstemmelse med tilsynsmæssige instrukser vedrørende brug og inkorporering af sådanne internationale standarder. Denne forordning dækker også integritet, sikkerhed og modstandsdygtighed i fysiske infrastrukturer og faciliteter, som understøtter brugen af teknologi og de relevante IKT-relaterede processer og relevante personer, som led i de digitale fodaftryk, som en finansiel enheds transaktioner efterlader.

Indberetning af IKT-relaterede hændelser (artikel 15-20)

Harmonisering og strømlining af indberetningen af IKT-relaterede hændelser opnås for det første gennem et krav til finansielle enheder om at fastlægge og gennemføre en styringsproces, der skal overvåge og registrere IKT-relaterede hændelser, efterfulgt af en forpligtelse til at klassificere dem på grundlag af kriterier, der er beskrevet nærmere i denne forordning, og som videreudvikles af ESA'erne gennem mandater for nærmere at angive væsentlighedstærskler. For det andet er det kun de IKT-relaterede hændelser, der betragtes som større, som skal indberettes til de kompetente myndigheder. Indberetningen bør behandles ved anvendelse af en fælles model og efter en harmoniseret procedure, således som den er udviklet af ESA'erne. Finansielle enheder bør indgive indledende, foreløbige og endelige rapporter og oplyse deres brugere og kunder om, hvor hændelser har eller kan få indflydelse på deres finansielle interesser. De kompetente myndigheder bør give relevante detaljer om hændelserne til andre institutioner eller myndigheder: til ESA'erne, til ECB og til de centrale kontaktpunkter, der er udpeget i henhold til direktiv (EU) 2016/1148.

For at starte en dialog mellem finansielle enheder og kompetente myndigheder, der kan bidrage til at mindske virkningerne og identificere passende løsninger, bør indberetningen af større IKT-relaterede hændelser suppleres af tilsynsmæssig feedback og vejledning.

Endelig bør muligheden for centralisering på EU-plan af indberetningen af IKT-relaterede hændelser undersøges yderligere i en fælles rapport fra ESA'erne, ECB og ENISA, hvori det vurderes, om det er muligt at oprette et fælles EU-knudepunkt for finansielle enheders indberetning af større IKT-relaterede hændelser.

Afprøvning af digital operationel modstandsdygtighed (artikel 21-24)

De kapaciteter og funktioner, der indgår rammen for IKT-risikostyring, skal regelmæssigt afprøves for beredskab i forhold til og identifikation af svagheder, mangler eller huller samt øjeblikkelig gennemførelse af korrigerende foranstaltninger. Denne forordning muliggør en forholdsmæssigt afpasset anvendelse af krav til afprøvning af digital operationel modstandsdygtighed, afhængigt af finansielle enheders størrelse, forretnings- og risikoprofiler: Mens alle enheder bør foretage en afprøvning af IKT-værktøjer og -systemer, er det kun de enheder, der af kompetente myndigheder (baseret på kriterierne i denne forordning og videreudviklet af ESA'erne) er udpeget som væsentlige og cybermodne, som

bør pålægges at foretage avanceret afprøvning baseret på trusselsbaserede penetrationstest (TLPT'er). Denne forordning fastsætter også krav til testere og anerkendelse af resultater af TLPT'er i hele Unionen for finansielle enheder, der har aktiviteter i flere medlemsstater.

IKT-tredjepartsrisici (artikel 25-39)

For det første er denne forordning udformet med henblik på at sikre en forsvarlig overvågning af IKT-tredjepartsrisici. Dette mål vil blive opfyldt gennem respekt for principbaserede regler, som finder anvendelse på finansielle enheders overvågning af risici, der opstår i forbindelse med tredjepartsudbydere af IKT-tjenester. For det andet harmoniserer denne forordning centrale elementer vedrørende tjenester, der leveres af tredjepartsudbydere af IKT-tjenester, og forholdet til disse. Disse elementer omfatter et minimum af aspekter, der betragtes som afgørende for at sætte den finansielle enhed i stand til at foretage en fuldstændig overvågning af IKT-tredjepartsrisici i løbet af indgåelses-, udførelses- og udløbsfasen i deres kontraktlige forhold og efter kontraktens udløb.

Navnlig skal de kontrakter, der regulerer det pågældende forhold, indeholde en fuldstændig beskrivelse af tjenester, angivelse af steder, hvor data skal behandles, fuldstændige beskrivelser af serviceniveauet ledsaget af kvantitative og kvalitative præstationsmål, relevante bestemmelser om adgang til, tilgængelighed, integritet og beskyttelse af personoplysninger samt sikkerhed i forbindelse med disse oplysninger, garantier for adgang, genopretning og tilbagesendelse i tilfælde af fejl forårsaget af tredjepartsudbydere af IKT-tjenester, opsigelsesvarsler og indberetningsforpligtelser for tredjepartsudbydere af IKT-tjenester, adgangsrettigheder, inspektion og revision foretaget af den finansielle enhed eller en udnævnt tredjepart, klare opsigelsesrettigheder og målrettede exitstrategier. Da nogle af disse kontraktlige elementer kan standardiseres, fremmer forordningen desuden en frivillig brug af standardkontraktbestemmelser, som skal udarbejdes med henblik på Kommissionens anvendelse af cloud computing-tjenester.

Endelig udgør forordningen et forsøg på at fremme konvergens i forbindelse med tilsynstilgange til IKT-tredjepartsrisici i den finansielle sektor ved at lade kritiske tredjepartsudbydere af IKT-tjenester omfatte af en EU-tilsynsramme. Gennem en ny harmoniseret lovramme tillægges den ESA, der er udnævnt som ledende tilsynsførende for hver af disse kritiske tredjepartsudbydere af IKT-tjenester, beføjelser til at sikre, at udbydere af digitale tjenester, der opfylder en vigtig rolle for at sikre en velfungerende finansiel sektor, overvåges i tilstrækkelig grad på paneuropæisk plan. Den tilsynsramme, der påtænkes i denne forordning, bygger på den eksisterende institutionelle arkitektur på området for finansielle tjenesteydelser, hvorved Det Fælles Udvalg af ESA'er sikrer koordinering på tværs af sektorer af alle anliggender, der vedrører IKT-risici, i overensstemmelse med dets opgaver vedrørerende cybersikkerhed og med støtte fra det relevante underudvalg (tilsynsforum), der udfører det forberedende arbejde med henblik på individuelle afgørelser og kollektive henstillinger til kritiske tredjepartsudbydere af IKT-tjenester.

Informationsudveksling (artikel 40)

For skabe bevidsthed om IKT-risici, minimere deres udbredelse, understøtte finansielle enheders forsvarskapaciteter og teknikker til detektion af trusler, giver denne forordning finansielle enheder mulighed for at indgå ordninger for indbyrdes udveksling af oplysninger og efterretninger om cybertrusler.

2020/0266 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 og (EU) nr. 909/2014

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Den Europæiske Centralbank[25],

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg[26],

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

(1) I den digitale tidsalder understøtter informations- og kommunikationsteknologi (IKT) komplekse systemer, der anvendes i forbindelse med hverdagens samfundsmæssige aktiviteter. Den sørger for, at vores økonomier fungerer i centrale sektorer, herunder finanssektoren, og at det indre marked fungerer bedre. Øget digitalisering og indbyrdes forbundethed forstærker også IKT-risici, der gør samfundet som helhed — og især det finansielle system — mere sårbart over for cybertrusler eller IKT-forstyrrelser. Allestedsnærværende brug af IKT-systemer og en høj grad af digitalisering og konnektivitet er i dag vigtige kendetegn ved alle aktiviteter i EU's finansielle enheder, men samtidig er digital modstandsdygtighed endnu ikke i tilstrækkeligt omfang indbygget i deres operationelle rammer.

(2) Brugen af IKT har i de seneste årti indtaget en central rolle inden for finans og har i dag kritisk relevans for driften af daglige funktioner i alle finansielle enheder. Digitalisering omfatter f.eks. betalinger, som i stigende grad er gået fra kontanter og

[25] [*henvisning tilføjes*] EUT C […] af […], s. […].
[26] [*henvisning tilføjes*] EUT C […] af […], s. […].

papirbaserede metoder til brugen af digitale løsninger, samt clearing og afvikling af værdipapirer, elektronisk og algoritmisk handel, låntagning og finansiering, peer-to-peer-finansiering, kreditvurdering, tegning af forsikringer, skadesbehandling og back office-funktioner. Finans er ikke kun blevet overvejende digital i hele sektoren, men digitalisering har også uddybet den indbyrdes forbundethed og afhængighed inden for den finansielle sektor og af tredjeparters infrastruktur og tredjepartsudbydere af tjenester.

(3) Det Europæiske Udvalg for Systemiske Risici (ESRB) bekræftede på ny i en rapport fra 2020 om systemiske cyberrisici[27], hvordan det eksisterende høje niveau af indbyrdes forbundethed blandt finansielle enheder, finansielle markeder og finansielle markedsinfrastrukturer, og navnlig deres IKT-systemers indbyrdes forbundethed, potentielt kan udgøre en systemisk sårbarhed, da lokaliserede cyberhændelser hurtigt kan sprede sig fra én af de ca. 22 000 finansielle enheder i EU[28] til hele det finansielle system, uhindret af geografiske grænser. Alvorlige IKT-relaterede overtrædelser i den finansielle sektor har ikke kun virkninger for finansielle enheder isoleret set. De baner også vejen for udbredelsen af lokaliserede sårbarheder på tværs af de finansielle transmissionskanaler og udløser potentielt negative konsekvenser for stabiliteten i EU's finansielle system, idet de skaber likviditetsudstrømning og et generelt tab af tillid og tiltroen til finansielle markeder.

(4) I de seneste år har nationale, europæiske og internationale politiske beslutningstagere, lovgivere og standardiseringsorganer sat fokus på IKT-risici i et forsøg på at øge modstandsdygtigheden, fastsætte standarder og koordinere det lovgivnings- og tilsynsmæssige arbejde. På internationalt plan sigter Baselkomitéen for Banktilsyn, Udvalget om Betalings- og Markedsinfrastrukturer, Rådet for Finansiel Stabilitet, Financial Stability Institute samt G7- og G20-landene mod at udstyre kompetente myndigheder og markedsoperatører på tværs af forskellige jurisdiktioner med værktøjer, der skal styrke deres finansielle systemers modstandsdygtighed.

(5) Til trods for målrettede politiske og lovgivningsmæssige initiativer på nationalt plan og EU-plan udgør IKT-risici fortsat en udfordring for den operationelle modstandsdygtighed, kapacitet og stabilitet i EU's finansielle system. Den reform, der fulgte efter den finansielle krise i 2008 styrkede primært den finansielle modstandsdygtighed i EU's finansielle sektor og sigtede mod at bevare EU's konkurrenceevne og stabilitet set fra et økonomisk, tilsyns- og markedsadfærdsmæssigt perspektiv. Selv om IKT-sikkerhed og digital modstandsdygtighed udgør dele af den operationelle risiko, har der været mindre fokus herpå i den lovgivningsmæssige dagsorden efter krisen, og de er kun blevet udviklet på nogle områder inden for EU's politik for finansielle tjenesteydelser og lovgivningsmæssige rammer eller kun i nogle få medlemsstater.

---

[27] Rapport fra Det Europæiske Udvalg for Systemiske Risici (ESRB) fra februar 2020 https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

[28] I henhold til den konsekvensanalyse, der ledsager den gennemgang, der er foretaget af de europæiske tilsynsmyndigheder (SWD(2017) 308), findes der ca. 5 665 kreditinstitutter, 5 934 investeringsselskaber, 2 666 forsikringsselskaber, 1 573 arbejdsmarkedsrelaterede pensionskasser, 2 500 kapitalforvaltningsselskaber, 350 markedsinfrastrukturer (såsom CCP'er, børser, systematiske internalisatorer, transaktionsregistre og MHF'er) 45 kreditvurderingsbureauer og 2 500 betalingsinstitutter og e-pengeinstitutter, der er meddelt tilladelse. Det giver i alt ca. 21 233 enheder og omfatter ikke crowdfundingenheder, revisorer og revisionsfirmaer, udbydere af kryptoaktivtjenester og benchmarkadministratorer.

(6) I Kommissionens fintechhandlingsplan fra 2018[29] fremhævedes den afgørende betydning af at gøre EU's finansielle sektor mere modstandsdygtig, også set fra et operationelt perspektiv, for at sikre dens teknologiske sikkerhed, og sikre, at den er velfungerende, at den hurtigt kan genoprettes efter IKT-relaterede overtrædelser og hændelser, som i sidste ende gør det muligt at udbyde finansielle tjenesteydelser på en effektiv og uproblematisk måde i hele EU, herunder i situationer med stresspåvirkning, samtidig med at forbrugernes og markedets tiltro og tillid bevares.

(7) I april 2019 udsendte Den Europæiske Banktilsynsmyndighed (EBA), Den Europæiske Værdipapir- og Markedstilsynsmyndighed (ESMA) og Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger (EIOPA) (som samlet betegnes "europæiske tilsynsmyndigheder" eller "ESA'er") i fællesskab to sæt teknisk rådgivning, hvori de opfordrede til en sammenhængende tilgang til IKT-risici inden for finans og henstillede til på en forholdsmæssigt afpasset måde at styrke den digitale operationelle modstandsdygtighed i sektoren for finansielle tjenesteydelser gennem et sektorspecifikt EU-initiativ.

(8) EU's finansielle sektor er omfattet af et harmoniseret fælles regelsæt og er reguleret i henhold til et europæisk finanstilsynssystem. Ikke desto mindre er håndteringen af digital operationel modstandsdygtighed og IKT-sikkerhed endnu ikke harmoniseret på fyldestgørende eller konsekvent vis, og det til trods for, at digital operationel modstandsdygtighed er yderst vigtig for at sikre finansiel stabilitet og markedsintegritet i den digitale tidsalder og ikke er mindre vigtig end f.eks. fælles standarder for tilsyn og markedsadfærd. Det fælles regelsæt og tilsynssystemet bør derfor udvikles med henblik på også at omfatte denne komponent, idet mandatet for de finansielle tilsynsmyndigheder, som har til opgave at overvåge og beskytte den finansielle stabilitet og markedsintegriteten, udvides.

(9) Lovgivningsmæssige forskelle og uensartede nationale regulerings- eller tilsynsmæssige tilgange til IKT-risici udløser hindringer for det indre marked for finansielle tjenesteydelser, som igen hæmmer en problemfri udøvelse af den frie etableringsret og af retten til fri udveksling af tjenesteydelser. Konkurrencen mellem samme type af finansielle enheder, som har aktiviteter i forskellige medlemsstater, risikerer ligeledes at blive fordrejet. Navnlig på de områder, hvor EU-harmonisering har været meget begrænset eller ikke-eksisterende — såsom henholdsvis afprøvning af digital operationel modstandsdygtighed og overvågning af IKT-tredjepartsrisici — kan forskelle, der skyldes en påtænkt udvikling på nationalt plan, udløse yderligere hindringer for et velfungerende indre marked til skade for markedsdeltagere og den finansielle stabilitet.

(10) Den delvise måde, hvorpå bestemmelser vedrørende IKT-risici hidtil er blevet håndteret på EU-plan, medfører huller eller overlapninger på vigtige områder, f.eks. indberetning af IKT-relaterede hændelser og afprøvning af digital operationel modstandsdygtighed, og skaber uoverensstemmelser, som udspringer af nye divergerende nationale regler eller omkostningsineffektiv anvendelse af overlappende regler. Dette er særligt skadeligt for en IKT-intensiv bruger som den finansielle sektor,

---

[29] Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Den Europæiske Centralbank, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget, Fintechhandlingsplan for en mere konkurrencedygtig og innovativ finanssektor i Europa (COM(2018) 109 final), https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

da teknologiske risici er grænseoverskridende og den finansielle sektor udruller sine tjenesteydelser på et bredt grænseoverskridende grundlag inden for og uden for EU.

Individuelle finansielle enheder, som har aktiviteter på et grænseoverskridende grundlag, eller som er indehavere af flere tilladelser (f.eks. kan én finansiel enhed have tilladelser til henholdsvis at udøve bankvirksomhed, udøve virksomhed som investeringsselskab og betalingsinstitut, som hver især er meddelt af en forskellig kompetent myndighed i en eller flere medlemsstater), står over for operationelle udfordringer i forbindelse med at imødegå IKT-risici og afbøde negative virkninger af IKT-hændelser på egen hånd og på en sammenhængende omkostningseffektiv måde.

(11) Da det fælles regelsæt ikke ledsages af en udførlig IKT-ramme eller ramme for operationelle risici, er der behov for yderligere harmonisering af centrale krav til digital operationel modstandsdygtighed for alle finansielle enheder. De kapaciteter og den overordnede modstandsdygtighed, som finansielle enheder med udgangspunkt i sådanne centrale krav skal udvikle for at modstå operationelle driftstop, vil bidrage til at bevare stabiliteten og integriteten på EU's finansielle markeder og dermed bidrage til at sikre et højt beskyttelsesniveau for investorer og forbrugere i EU. Da denne forordning har til formål at bidrage til et velfungerende indre marked, bør den bygge på bestemmelserne i artikel 114 i TEUF som fortolket i overensstemmelse med EU-Domstolens faste praksis.

(12) Denne forordning har for det første til formål at konsolidere og ajourføre de krav til IKT-risici, som hidtil er blevet behandlet separat i de forskellige forordninger og direktiver. EU's retsakter omfattede rigtigt nok hovedkategorierne af finansielle risici (f.eks. kreditrisiko, markedsrisiko, modpartskreditrisiko og likviditetsrisiko, risiko forbundet med markedsadfærd), men på tidspunktet for deres vedtagelse kunne de ikke tackle alle de komponenter, der indgår i operationel modstandsdygtighed, på fyldestgørende vis. Kravene til operationelle risici, når de behandles yderligere i disse EU-retsakter, begunstiger ofte en traditionel kvantitativ tilgang til risikohåndtering (navnlig ved at fastsætte et kapitalkrav til at dække IKT-risici), frem for at fastsætte målrettede kvalitative krav, der skal fremme kapaciteter ved hjælp af krav med sigte på beskyttelses-, detektions-, inddæmnings-, genopretnings- og reparationskapaciteter som værn mod IKT-risici, eller ved hjælp af indførelse af indberetningskapaciteter og digitale afprøvningskapaciteter. Hensigten med disse direktiver og forordninger var primært at dække væsentlige regler om tilsyn, markedsintegritet eller -adfærd.

Med udformningen af denne forordning, som konsoliderer og ajourfører regler om IKT-risici, vil alle bestemmelser om digitale risici i den finansielle sektor for første gang blive samlet på en konsekvent måde i én enkelt lovgivningsmæssig retsakt. Dette initiativ bør således udfylde hullerne eller afhjælpe uoverensstemmelserne i nogle af de nævnte retsakter, herunder med hensyn til den heri anvendte terminologi, og bør eksplicit henvise til IKT-risici gennem målrettede regler om kapaciteter til IKT-risikostyring, indberetning og afprøvning samt overvågning af tredjepartsrisici.

(13) Finansielle enheder bør følge den samme tilgang og de samme principbaserede regler, når de imødegår IKT-risici. Konsekvens bidrager til at øge tilliden til det finansielle system og bevare dets stabilitet, navnlig i tider med overforbrug af IKT-systemer, platforme og infrastrukturer, hvilket medfører øgede digitale risici.

Respekten for en grundlæggende cyberhygiejne skal også hindre, at økonomien påføres store omkostninger ved at minimere virkningerne af og omkostningerne i forbindelse med IKT-forstyrrelser,

(14) Anvendelsen af en forordning hjælper til at mindske reguleringsmæssig kompleksitet, fremme tilsynsmæssig konvergens og øge retssikkerheden, samtidig med at den bidrager til at begrænse overholdelsesomkostninger, navnlig for finansielle enheder, der har aktiviteter på tværs af grænserne, og til at mindske konkurrenceforvridninger. Valget af en forordning i forbindelse med udarbejdelsen af en fælles ramme for digital operationel modstandsdygtighed i finansielle enheder synes derfor at være den mest hensigtsmæssige metode til at sikre en homogen og sammenhængende anvendelse af alle de komponenter, der indgår i IKT-risikostyring i EU's finansielle sektorer.

(15) Foruden lovgivningen om finansielle tjenesteydelser, udgør Europa-Parlamentets og Rådets direktiv (EU) 2016/1148[30] den nuværende overordnede ramme for cybersikkerhed på EU-plan. Blandt de syv kritiske sektorer, finder nævnte direktiv også finder anvendelse på tre typer af finansielle enheder, nemlig kreditinstitutter, markedspladser og centrale modparter. Idet direktiv (EU) 2016/1148 fastsætter en mekanisme til identifikation på nationalt plan af operatører af væsentlige tjenester, er det i imidlertid kun visse kreditinstitutter, markedspladser og centrale modparter, der er udpeget af medlemsstater, som i praksis medtages under dette anvendelsesområde, og som dermed skal overholde de heri fastsatte krav til IKT-risici og indberetning af hændelser.

(16) Da denne forordning højner niveauet af harmonisering af de komponenter, der indgår i digital modstandsdygtighed, ved at indføre krav til IKT-risikostyring og indberetning af IKT-relaterede hændelser, som er strengere end de krav, der er fastlagt i den nuværende EU-lovgivning om finansielle tjenesteydelser, udgør dette ligeledes en øget harmonisering i sammenligning med de krav, der er fastlagt i direktiv (EU) 2016/1148. Derfor udgør denne forordning en særlig lovregel i forhold til direktiv (EU) 2016/1148.

Det er yderst vigtigt at bevare en tæt forbindelse mellem den finansielle sektor og EU's horisontale ramme for cybersikkerhed, da dette vil sikre sammenhæng med de strategier om cybersikkerhed, som medlemsstaterne allerede har vedtaget, og give de finansielle tilsynsmyndigheder mulighed for at få kendskab til cyberhændelser, der har virkninger for de øvrige sektorer, som er omfattet af direktiv (EU) 2016/1148.

(17) For at muliggøre en grænseoverskridende læringsproces og effektivt at udnytte andre sektorers erfaringer med håndtering af cybertrusler bør finansielle enheder som omhandlet i direktiv (EU) 2016/1148 fortsat indgå i det nævnte direktivs "økosystem" (f.eks. NIS-samarbejdsgruppen og CSIRT'er).

Både ESA'er og nationale kompetente myndigheder bør have mulighed for at deltage i henholdsvis de strategiske politiske drøftelser og det tekniske arbejde i NIS-samarbejdsgruppen, udveksle oplysninger og samarbejde yderligere med de centrale kontaktpunkter, der er udpeget i henhold til direktiv (EU) 2016/1148. De kompetente

[30] Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

myndigheder i henhold til denne forordning bør også rådføre sig med og samarbejde med de nationale CSIRT'er, der er udpeget i overensstemmelse med artikel 9 i direktiv (EU) 2016/1148.

(18) Dette er også vigtigt for at sikre overensstemmelse med direktivet om europæisk kritisk infrastruktur, som i øjeblikket revideres for at styrke beskyttelsen af og modstandsdygtigheden i kritiske infrastrukturer mod ikke-cyberrelaterede trusler, med mulige konsekvenser for den finansielle sektor[31].

(19) Udbydere af cloud computing-tjenester er en kategori af udbydere af digitale tjenester, som er omfattet af direktiv (EU) 2016/1148. Som sådan er de underlagt efterfølgende tilsyn, som udføres af de nationale myndigheder udpeget i henhold til nævnte direktiv, og som er begrænset til de krav til IKT-sikkerhed og indberetning af hændelser, der er fastlagt i nævnte retsakt. Da den tilsynsramme, der fastlægges ved denne forordning, finder anvendelse på alle kritiske tredjepartsudbydere af IKT-tjenester, herunder udbydere af cloud computing-tjenester, når de udbyder IKT-tjenester til finansielle enheder, bør den betragtes som et supplement til det tilsyn, der finder sted i henhold til direktiv (EU) 2016/1148. Derudover bør den tilsynsramme, der fastlægges ved denne forordning, omfatte udbydere af cloud computing-tjenester, idet der ikke findes en horisontal sektorneutral EU-ramme, der opretter en digital tilsynsmyndighed.

(20) For at bevare den fulde kontrol med IKT-risici skal finansielle enheder have indført omfangsrige kapaciteter, der muliggør en forsvarlig og effektiv IKT-risikostyring, sammen med specifikke mekanismer og politikker med henblik på indberetning af IKT-relaterede hændelser, afprøvning af IKT-systemer, -kontroller og -processer samt på håndtering af IKT-tredjepartsrisici. Standarden for digital operationel modstandsdygtighed i det finansielle system bør højnes, samtidig med at der skabes mulighed for en forholdsmæssigt afpasset anvendelse af krav til finansielle enheder, som er mikrovirksomheder som defineret i Kommissionens henstilling 2003/361/EF[32].

(21) Tærskler og klassificeringssystemer vedrørende indberetning af IKT-relaterede hændelser varierer væsentligt på nationalt plan. Mens der sandsynligvis kan opnås enighed gennem det relevante arbejde, der udføres af Den Europæiske Unions Agentur for Cybersikkerhed (ENISA)[33] og NIS-samarbejdsgruppen, med hensyn til de finansielle enheder, der er omfattet af direktiv (EU) 2016/1148, findes der stadig eller kan der opstå divergerende tilgange til tærskler og klassificeringssystemer for de resterende finansielle enheder. Dette medfører, at finansielle enheder skal rette sig efter flere krav, navnlig når de operer på tværs af flere EU-jurisdiktioner, og når de er del af en finansiel koncern. Disse forskelle kan hindre indførelsen af yderligere ensartede eller centraliserede EU-mekanismer, der fremskynder indberetningsprocessen og understøtter en hurtig og problemfri informationsudveksling mellem kompetente myndigheder, hvilket er yderst vigtigt for

---

31 Rådets direktiv 2008/114/EF af 8. december 2008 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre (EUT L 345 af 23.12.2008, s. 75).

32 Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).

33 ENISA Reference Incident Classification Taxonomy, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

imødegåelsen af IKT-risici i tilfælde af storstilede angreb med potentielle systemiske konsekvenser til følge.

(22) For at sætte kompetente myndigheder i stand til opfylde deres tilsynsmæssige roller ved at opnå et fuldstændigt overblik over IKT-relaterede hændelsers karakter, frekvens, betydning og virkninger og for at styrke informationsudvekslingen mellem relevante offentlige myndigheder, herunder retshåndhævende myndigheder og afviklingsmyndigheder, er det nødvendigt at fastlægge regler for, at fuldføre ordningen for indberetning af IKT-hændelser med de krav, der på nuværende tidspunkt mangler i lovgivning om finansielle delsektorer, og fjerne eksisterende overlapninger og duplikationer for at mindske omkostningerne. Det er derfor vigtigt at harmonisere ordningen for indberetning af IKT-hændelser ved at pålægge alle finansielle enheder at indberette udelukkende til deres kompetente myndigheder. ESA'erne bør desuden tillægges beføjelse til yderligere at præcisere elementer vedrørende indberetning af IKT-hændelser, f.eks. klassificeringssystemer, tidsrammer, datasæt, modeller og gældende tærskler.

(23) Krav til afprøvning af digital operationel modstandsdygtighed er blevet udviklet i nogle finansielle delsektorer inden for adskillige og ukoordinerede nationale rammer, som på forskellig vis omhandler de samme spørgsmål. Dette fører til duplikation af omkostninger for grænseoverskridende finansielle enheder og vanskeliggør den gensidige anerkendelse af resultater. Ukoordineret afprøvning kan derfor segmentere det indre marked.

(24) Når afprøvning ikke er påkrævet, vil sårbarheder fortsat ikke blive detekteret, hvilket desuden udsætter de finansielle enheder og i sidste ende stabiliteten og integriteten i den finansielle sektor for en højere risiko. Uden en indsats på EU-plan vil afprøvning af digital operationel modstandsdygtighed fortsat være uensartet, og der vil ikke være nogen gensidig anerkendelse af testresultater på tværs af de forskellige jurisdiktioner. Da det er usandsynligt, at andre finansielle delsektorer vil indgå sådanne ordninger i et meningsfuldt omfang, vil de desuden gå glip af de potentielle fordele, f.eks. detektion af sårbarheder og risici, kapaciteter til forsvarsafprøvning og driftsstabilitet, og større tiltro blandt kunder, leverandører og forretningspartnere. For at afhjælpe sådanne overlapninger, forskelle og huller er det nødvendigt at fastlægge regler, der har til formål at koordinere den afprøvning, som finansielle enheder og kompetente myndigheder foretager, og dermed lette den gensidige anerkendelse af avanceret afprøvning for signifikante finansielle enheder.

(25) Finansielle enheders afhængighed af IKT-tjenester skyldes delvist deres behov for at tilpasse sig en ny konkurrencepræget digital og global økonomi og for at fremme deres forretningseffektivitet og imødekomme forbrugerefterspørgslen. Karakteren og omfanget af en sådan afhængighed har gennemgået en løbende udvikling i de senere år og har medført mindre finansiel formidling, muliggjort ekspansion og skalerbarhed af virksomheder i forbindelse med udrulningen af finansielle aktiviteter, samtidig med at der udbydes en bred vifte af IKT-værktøjer til styring af komplekse interne processer.

(26) Denne vidtgående anvendelse af IKT-tjenester dokumenteres ved komplekse kontraktlige ordninger, i forbindelse med hvilke finansielle enheder ofte støder på vanskeligheder med at forhandle kontraktvilkår, der er tilpasset til den tilsynsmæssige standard eller andre reguleringsmæssige krav, som de er omfattet af, eller på anden måde med at håndhæve specifikke rettigheder, f.eks. adgangs- eller

revisionsrettigheder, når sidstnævnte er fastsat i aftalerne. Mange af sådanne kontrakter indeholder desuden ikke tilstrækkelige garantier, som muliggør en fuldgyldig overvågning af underentrepriseforhold, og berøver dermed den finansielle enhed for dens mulighed for at vurdere disse dertil knyttede risici. Dertil kommer, at sådanne kontrakter ikke altid i tilstrækkeligt omfang tager højde for individuelle eller specifikke behov blandt aktører i den finansielle sektor, da tredjepartsudbydere af IKT-tjenester ofte udbyder standardiserede tjenester til forskellige kundetyper.

(27) På trods af visse generelle regler om outsourcing i nogle EU-retsakterne om finansielle tjenesteydelser er overvågningen af den kontraktlige dimension ikke fuldt ud forankret i EU-lovgivningen. I mangel af klare og skræddersyede EU-standarder, som finder anvendelse på de kontraktlige ordninger, der indgås med tredjepartsudbydere af IKT-tjenester, er der ikke på fyldestgørende vis taget højde for den eksterne kilde til IKT-risici. Derfor er det nødvendigt at fastsætte visse nøgleprincipper, der skal fungere som rettesnor for finansielle enheders styring af IKT-tredjepartsrisici, og som ledsages af et sæt centrale kontraktlige rettigheder i forhold til flere elementer af kontraktopfyldelse og -opsigelse med henblik på at fastsætte visse minimumsgarantier, der understøtter finansielle enheders evne til effektivt at overvåge alle de risici, der opstår hos IKT-tredjeparter.

(28) Der er en mangel på homogenitet og konvergens i forbindelse med IKT-tredjepartsrisici og afhængighed af IKT-tredjeparter. På trods af visse bestræbelser på at tackle det specifikke område outsourcing med udgangspunkt i henstillingerne fra 2017 om outsourcing til udbydere af cloud computing-tjenester[34], tages der i EU-lovgivningen knap nok højde for den problematik, der er forbundet med systemiske risici, som kan udløses af den finansielle sektors eksponering for et begrænset antal kritiske tredjepartsudbydere af IKT-tjenester. Denne mangel på EU-plan forværres af manglen på specifikke mandater og værktøjer, som giver nationale tilsynsmyndigheder mulighed for at opnå en god forståelse for afhængigheden af IKT-tredjeparter og foretage en tilstrækkelig overvågning af risici, der opstår som følge af koncentrationer af en sådan afhængighed af IKT-tredjeparter.

(29) Idet der tages hensyn til de potentielle systemiske risici, som den øgede anvendelse af outsourcing og koncentration af IKT-tredjepartsafhængighed medfører, og idet der hersker bevidsthed om utilstrækkeligheden af nationale mekanismer, som sætter finansielle tilsynsmyndigheder i stand til at kvantificere, kvalificere og afhjælpe de konsekvenser af IKT-risici, der opstår hos kritiske tredjepartsudbydere af IKT-tjenester, er det nødvendigt at fastlægge en passende EU-tilsynsramme , som gør det muligt at foretage løbende overvågning af aktiviteter hos tredjepartsudbydere af IKT-tjenester, som er kritiske udbydere til finansielle enheder.

(30) I takt med at IKT-trusler bliver mere komplekse og sofistikerede, afhænger gode detektions- og forebyggelsesforanstaltninger i høj grad af regelmæssig udveksling af trussels- og sårbarhedsefterretninger blandt finansielle enheder. Informationsudveksling bidrager til øget bevidsthed om cybertrusler, hvilket igen styrker finansielle enheders evne til at forhindre trusler i at blive til faktiske hændelser og sætter finansielle enheder i stand til bedre at inddæmme virkningerne af IKT-

[34] Henstillinger om outsourcing til udbydere af cloud computing-tjenester (EBA/REC/2017/03), som nu er ophævet af EBA's retningslinjer om outsourcing (EBA/GL/2019/02).

relaterede hændelser og foretage en mere effektiv genopretning. Da der ikke findes nogen retningslinjer på EU-plan, synes flere faktorer at have hæmmet en sådan udveksling af efterretninger, navnlig usikkerhed omkring foreneligheden med databeskyttelsesregler, antitrustregler og regler om ansvar.

(31) Dertil kommer, at tvivl med hensyn til den type oplysninger, som kan udveksles med en anden markedsdeltager eller med ikke-tilsynsmyndigheder (f.eks. ENISA, som analytisk input, eller Europol, med henblik på retshåndhævelse), medfører, at nyttige oplysninger tilbageholdes. Omfanget og kvaliteten af informationsudveksling er fortsat begrænset og fragmenteret, da de relevante udvekslinger primært finder sted lokalt (gennem nationale initiativer), og der findes ingen konsekvente ordninger for informationsudveksling på EU-plan, som er skræddersyet til behovene i en integreret finansiel sektor.

(32) Finansielle enheder bør derfor tilskyndes til i fællesskab at øge deres individuelle viden og praktiske erfaring på strategisk, taktisk og operationelt plan med henblik på at styrke deres kapaciteter til i tilstrækkeligt omfang at vurdere, overvåge, sikre forsvar mod og en indsats over for cybertrusler. Det er således nødvendigt at muliggøre indførelsen på EU-plan af mekanismer med henblik på frivillige ordninger for informationsudveksling, som, når de gennemføres i pålidelige miljøer, vil hjælpe finansverdenen til at forebygge og i fællesskab sikre en indsats over for trusler ved hurtigt at begrænse spredningen af IKT-risici og hindre potentiel afsmitning på tværs af de finansielle kanaler. Disse mekanismer bør gennemføres i fuld overensstemmelse med de gældende regler i EU's konkurrenceret[35] samt på en måde, der garanterer fuld overholdelse af EU's databeskyttelsesregler, navnlig Europa-Parlamentets og Rådets forordning (EU) 2016/679[36], og navnlig i forbindelse med behandling af personoplysninger, som er nødvendig med henblik på den legitime interesse, som forfølges af den dataansvarlige eller af tredjemand, jf. nævnte forordnings artikel 6, stk. 1, litra f).

(33) Til trods for den brede dækning, der påtænkes i denne forordning, bør der ved anvendelse af reglerne om digital operationel modstandsdygtighed tages hensyn til væsentlige forskelle mellem finansielle enheder med hensyn til størrelse, forretningsprofiler eller eksponering for digitale risici. Som et overordnet princip bør de finansielle enheder, når de afsætter ressourcer og kapaciteter til gennemførelsen af rammen for IKT-risikostyring, nøje afveje deres IKT-relaterede behov i forhold til deres størrelse og forretningsprofil, mens de kompetente myndigheder fortsat bør vurdere og se nærmere på tilgangen til en sådan afvejning.

(34) Da større finansielle enheder kan have adgang til flere ressourcer og hurtigt kan afsætte midler til at udvikle ledelsesstrukturer og indføre forskellige virksomhedsstrategier, er det kun finansielle enheder, der ikke er mikrovirksomheder som defineret i denne forordning, som skal pålægges at indføre mere komplekse ledelsesordninger. Sådanne enheder er bedre rustet til at indføre særlige

---

35 Kommissionens meddelelse — Retningslinjer for anvendelsen af artikel 101 i traktaten om Den Europæiske Unions funktionsmåde på horisontale samarbejdsaftaler (EUT C 11 af 14.1.2011, s. 1).

36 Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

ledelsesfunktioner med henblik på tilsynsordninger med tredjepartsudbydere af IKT-risici eller til at varetage krisestyring, til at tilrettelægge deres egen IKT-risikostyring efter modellen med tre forsvarslinjer eller til at vedtage et HR-dokument med en udførlig redegørelse for politikker vedrørende adgangsrettigheder.

På samme måde er det kun sådanne finansielle enheder, der bør opfordres til at foretage tilbundsgående vurderinger efter større ændringer af infrastrukturer og processer for net- og informationssystemer, regelmæssigt at foretage risikoanalyser af nedarvede IKT-systemer eller udvide afprøvningen af driftsstabiliteten samt indsats- og genopretningsplaner for at tegne et billede af overgangsscenarier mellem den primære IKT-infrastruktur og redundante faciliteter.

(35) Da kun de finansielle enheder, der er udpeget som væsentlige med henblik på avanceret afprøvning af digital modstandsdygtighed, bør pålægges at foretage trusselsbaserede penetrationstest, bør de administrative processer og finansielle omkostninger, som gennemførelsen af sådanne test indebærer, desuden overdrages til en lille procentdel af finansielle enheder. Med det formål at lette den reguleringsmæssige byrde er det endelig kun finansielle enheder, som ikke er mikroenheder, der bør anmodes om regelmæssigt at aflægge rapport til de kompetente myndigheder om alle omkostninger og tab, der forårsages af IKT-forstyrrelser, og resultaterne af gennemgange efter hændelser med væsentlige IKT-forstyrrelser.

(36) For at sikre fuld tilpasning af og overordnet konsekvens mellem finansielle enheders virksomhedsstrategier på den ene side og gennemførelse af IKT-risikostyring på den anden side bør ledelsesorganet pålægges fortsat at indtage en central og aktiv rolle i styringen og tilpasningen af rammen for IKT-risikostyring og den samlede strategi for digital modstandsdygtighed. Den tilgang, som ledelsesorganet skal anlægge, bør ikke kun fokusere på midlerne til at sikre modstandsdygtighed i IKT-systemer, men bør også omfatte mennesker og processer gennem en række politikker, som på hvert virksomhedsniveau og for alt personale fremmer stor bevidsthed om cybersikkerhed og et tilsagn om at respektere en streng cyberhygiejne på alle niveauer.

Ledelsesorganets endelig ansvar for styringen af en finansiel enheds IKT-risici bør være det overordnede princip i denne omfangsrige tilgang, der skal udmøntes yderligere i ledelsesorganets fortsatte indsats for at føre kontrol med overvågningen af IKT-risikostyring.

(37) Desuden går fuld ansvarliggørelse af ledelsesorganet hånd i hånd med sikring af et vist niveau af IKT-investeringer og et samlet budget for den pågældende finansielle enhed, således at den kan opnå en grundlæggende digital operationel modstandsdygtighed.

(38) Med inspiration fra relevante standarder, retningslinjer, henstillinger eller tilgange, der er fastlagt på internationalt og nationalt plan samt på sektorplan, vedrørende styring af cyberrisici[37] fremmer denne forordning et sæt funktioner, der gør det lettere foretage

[37] CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, https://www.bis.org/cpmi/publ/d146.pdf G7 *Fundamental Elements of Cybersecurity for the Financial Sector,* https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; NIST Cybersecurity Framework, https://www.nist.gov/cyberframework; FSB *CIRR toolkit*, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

en overordnet strukturering af IKT-risikostyring. Så længe de hovedkapaciteter, som finansielle enheder indfører, opfylder de behov, der er knyttet til de planlagte mål for de funktioner (identifikation, beskyttelse og forebyggelse, detektion, indsats og genopretning, læring og udvikling og kommunikation), som er omhandlet i denne forordning, står det finansielle enheder frit for at anvende modeller for IKT-risikostyring, som er udformet eller kategoriseret på en anden måde.

(39) For at holde trit med et cybertrusselsbillede i udvikling bør finansielle enheder opretholde opdaterede IKT-systemer, der er pålidelige og udstyret med tilstrækkelig kapacitet til ikke kun at garantere databehandling, alt efter hvad der er nødvendigt for gennemførelsen af deres tjenester, men også for at sikre teknologisk modstandsdygtighed, der gør det muligt for finansielle enheder i tilstrækkelig grad at tackle yderligere behandlingsrelaterede behov, som stressede markedsforhold eller andre vanskelige situationer kan give anledning til. Denne forordning indebærer ikke nogen standardisering af specifikke IKT-systemer, -værktøjer eller -teknologier, men beror på finansielle enheders passende anvendelse af europæiske og internationalt anerkendte tekniske standarder (f.eks. ISO) eller bedste praksis i sektoren, for så vidt som en sådan anvendelse er i fuld overensstemmelse med specifikke tilsynsmæssige instrukser vedrørende brug og inkorporering af sådanne internationale standarder.

(40) Effektive planer for driftsstabilitet og genopretningsplaner er påkrævet, således at finansielle enheder omgående og hurtigt kan finde en løsning på IKT-relaterede hændelser, navnlig cyberangreb, ved at begrænse skaden og prioritere genoptagelsen af aktiviteter og genopretningstiltag. Mens backup-systemer uden unødigt ophold bør påbegynde behandlingen, bør en sådan påbegyndelse dog på ingen måde bringe net- og informationssystemers integritet og sikkerhed eller datafortroligheden i fare.

(41) Mens denne forordning giver finansielle enheder mulighed for at fastsætte mål for genopretningstiden på en fleksibel måde og dermed fastsætte sådanne mål under fuld hensyntagen til den relevante funktions karakter og kritiske betydning og eventuelle specifikke forretningsmæssige behov, bør der også kræves en vurdering af den potentielle samlede indvirkning på markedseffektiviteten, når sådanne mål fastsættes.

(42) De væsentlige konsekvenser af cyberangreb forstærkes, når de finder sted i den finansielle sektor, som er et område, der er i langt større fare for at blive mål for ondsindede formidlere, som forsøger at opnå finansielle gevinster direkte fra kilden. For at afbøde sådanne risici og for at forhindre, at IKT-systemer mister deres integritet eller bliver utilgængelige, at der sker overtrædelser af datafortroligheden, eller at fysiske IKT-infrastrukturer skades, bør finansielle enheders indberetning af større IKT-relaterede hændelser forbedres væsentligt.

Indberetningen af IKT-relaterede hændelser bør harmoniseres for alle finansielle enheder ved at pålægge dem udelukkende at foretage indberetning til deres kompetente myndigheder. Mens alle finansielle enheder vil være omfattet af denne indberetning, bør de ikke alle berøres heraf på samme måde, da relevante væsentlighedstærskler og tidsrammer bør kalibreres til kun at tage højde for større IKT-relaterede hændelser. Direkte indberetning vil give finansielle tilsynsmyndigheder adgang til oplysninger om IKT-relaterede hændelser. Ikke desto mindre bør finansielle tilsynsmyndigheder videreformidle disse oplysninger til ikke-finansielle offentlige myndigheder (kompetente NIS-myndigheder, nationale databeskyttelsesmyndigheder og retshåndhævende myndigheder ved hændelser af

kriminel karakter). Oplysningerne om den IKT-relaterede hændelser bør sendes begge veje: De finansielle tilsynsmyndigheder bør give al nødvendig feedback eller vejledning til den finansielle enhed, mens ESA'erne bør dele anonymiserede data om trusler og sårbarheder forbundet med en hændelse for at bidrage til det bredere kollektive forsvar.

(43) Yderligere overvejelser vedrørende en mulig centralisering af indberetninger af IKT-relaterede hændelser bør påtænkes ved hjælp af et fælles centralt EU-knudepunkt, som enten direkte modtager de relevante indberetninger og automatisk underretter nationale kompetente myndigheder, eller som blot centraliserer indberetninger, som de nationale kompetente myndigheder har indgivet, og varetager en koordinatorrolle. Det bør pålægges ESA'erne i samråd med ECB og ENISA inden en nærmere fastsat dato at udarbejde en fælles rapport, hvori det undersøges, om det er praktisk muligt at oprette et sådant centralt EU-knudepunkt.

(44) For at opnå en forsvarlig digital operationel modstandsdygtighed og skabe overensstemmelse med international standarder (f.eks. *G7 Fundamental Elements for Threat-Led Penetration Testing*) bør finansielle enheder regelmæssigt afprøve deres IKT-systemer og teste deres IKT-medarbejdere med hensyn til effektiviteten af deres forebyggelses-, detektions-, indsats- og genopretningskapaciteter for at afsløre og afhjælpe potentielle IKT-sårbarheder. For at sætte ind over for forskelle på tværs af og inden for de finansielle delsektorer, som vedrører de finansielle enheders cybersikkerhedsberedskab, bør afprøvning omfatte en bred vifte af værktøjer og tiltag, der spænder lige fra en vurdering af grundlæggende krav (f.eks. sårbarhedsvurderinger og -scanninger, analyser af open source software, vurderinger af netsikkerhed, analyser af huller, fysiske sikkerhedsgennemgange, spørgeskemaer og løsninger til scanningssoftware, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitettest, præstationstest eller end-to-end-test) til mere avanceret afprøvning (f.eks. TLPT for de finansielle enheder, der set fra et IKT-perspektiv er modne nok til at kunne foretage sådanne test). Afprøvning af digital operationel modstandsdygtighed bør således være mere krævende for væsentlige finansielle enheder (f.eks. store kreditinstitutter, børser, centrale værdipapircentraler, centrale modparter osv.). Samtidig er afprøvning af digital operationel modstandsdygtighed også mere relevant for visse delsektorer, som varetager en systemisk rolle (f.eks. betalinger, bankvirksomhed, clearing og afvikling), og mindre relevant for andre delsektorer (f.eks. kapitalforvaltere, kreditvurderingsbureauer osv.). Grænseoverskridende finansielle enheder, der udøver deres frie etableringsret og ret til fri udveksling af tjenesteydelser i EU, bør opfylde et fælles sæt avancerede afprøvningskrav (f.eks. TLPT) i deres hjemland, og en sådan test bør inkludere IKT-infrastrukturerne i alle jurisdiktioner, hvor den grænseoverskridende koncern opererer inden for EU, og dermed give grænseoverskridende koncerner mulighed for kun at pådrage sig omkostninger i én jurisdiktion.

(45) For at sikre en forsvarlig overvågning af IKT-tredjepartsrisici er det nødvendigt at fastlægge en række principbaserede regler, der skal fungere som rettesnor for finansielle enheders overvågning af risici i forbindelse med funktioner, der outsources til tredjepartsudbydere af IKT-tjenester, og mere generelt i forbindelse med afhængighed af IKT-tredjeparter.

(46) En finansiel enhed bør til enhver tid fortsat være ansvarlig for opfyldelsen af forpligtelser i henhold til denne forordning. En forholdsmæssigt afpasset overvågning

af risici, som opstår hos tredjepartsudbyderen af IKT-tjenester, bør tilrettelægges under behørig hensyntagen til omfanget, kompleksiteten og betydningen af den IKT-relaterede afhængighed eller tjenesternes kritiske karakter eller betydning, processer eller funktioner, der er omfattet af de kontraktlige ordninger, og i sidste ende på grundlag af en omhyggelig vurdering af en eventuel potentiel indvirkning på kvaliteten af finansielle tjenesteydelser og deres stabilitet på individuelt plan og koncernplan, alt efter hvad der er relevant.

(47) Fuldførelsen af en sådan overvågning bør følge en strategisk tilgang til IKT-tredjepartsrisici, der formaliseres ved, at den finansielle enheds ledelsesorgan vedtager en målrettet strategi, som tager udgangspunkt i en løbende screening af enhver sådan afhængighed af IKT-tredjeparter. For at øge den tilsynsmæssige bevidsthed om afhængighed af IKT-tredjeparter og med henblik på yderligere at understøtte den tilsynsramme, der oprettes ved denne forordning, bør finansielle tilsynsmyndigheder regelmæssigt modtage væsentlige oplysninger fra registrene og bør have mulighed for anmode om uddrag herfra på ad hoc-basis.

(48) En grundig analyse forud for kontraktindgåelsen skal understøtte og gå forud for den formelle indgåelse af kontraktlige ordninger, samtidig med at kontraktopsigelse som minimum bør være foranlediget af en række omstændigheder, der påviser mangler hos tredjepartsudbyderen af IKT-tjenester.

(49) For at tackle de systemiske virkninger af den koncentrationsrisiko, der er forbundet med IKT-tredjeparter, bør der tilstræbes en afbalanceret løsning ved hjælp af en fleksibel og gradvis tilgang, da strenge lofter eller begrænsninger kan være en hindring for virksomhedsadfærd og kontraktfrihed. Finansielle enheder bør foretage en grundig vurdering af de kontraktlige ordninger for at identificere sandsynligheden for, at sådanne risici opstår, herunder ved hjælp af tilbundsgående analyser af ordninger for videreoutsourcing, navnlig når de er indgået med tredjepartsudbydere af IKT-tjenester med hjemsted i et tredjeland. På nuværende tidspunkt og med henblik på at finde en rimelig balance mellem nødvendigheden af at bevare kontraktfriheden og af at sikre den finansielle stabilitet anses det ikke for hensigtsmæssigt at fastsætte strenge lofter og begrænsninger for eksponeringen for IKT-tredjeparter. Den ESA, der er udpeget til at føre tilsyn med hver enkelt kritisk tredjepartsudbyder af IKT-tjenester ("ledende tilsynsførende"), bør i forbindelse med varetagelsen af tilsynsopgaver være særligt opmærksom på at opnå fuld forståelse for omfanget af den indbyrdes afhængighed og identificere særlige tilfælde, hvor en høj koncentrationsgrad af kritiske tredjepartsudbydere af IKT-tjenester i EU sandsynligvis vil lægge pres på stabiliteten og integriteten i EU's finansielle system, og bør fremme en dialog med kritiske tredjepartsudbydere af IKT-tjenester, hvor en sådan risiko er identificeret[38].

(50) For regelmæssigt at kunne vurdere og overvåge evnen hos tredjepartsudbydere af IKT-tjenester til sikkert at levere tjenester til den finansielle enhed, uden at dette har negative virkninger for dennes modstandsdygtighed, bør der foretages en harmonisering af centrale kontraktlige elementer under hele opfyldelsen af kontrakter med tredjepartsudbydere af IKT-tjenester. Disse elementer dækker kun et minimalt antal kontraktlige aspekter, som anses for afgørende for, at den finansielle enhed kan

[38] Hvis der opstår risiko for misbrug begået af en tredjepartsudbyder af IKT-tjenester, der betragtes som dominerende, bør finansielle enheder desuden også have mulighed for at indgive enten formelle eller uformelle klager til Europa-Kommissionen eller de nationale konkurrencemyndigheder.

foretage fuld overvågning med henblik på at sikre sin digitale modstandsdygtighed, som beror på IKT-tjenestens stabilitet og sikkerhed.

(51) Kontraktlige ordninger bør navnlig indeholde en specifikation bestående af komplette beskrivelser af funktioner og tjenester, af steder, hvor sådanne funktioner udføres, og hvor der behandles data, samt fuldstændige beskrivelser af serviceniveauet ledsaget af kvantitative og kvalitative præstationsmål inden for aftalte serviceniveauer, således at den finansielle enhed kan foretage en effektiv overvågning. I samme ånd bør bestemmelser om adgang, tilgængelighed, integritet, sikkerhed og beskyttelse af personoplysninger samt garantier for adgang, genopretning og tilbagesendelse i tilfælde af insolvens eller afvikling, eller i tilfælde af at tredjepartsudbyderen af IKT-tjenester afbryder sine forretningsaktiviteter, også betragtes som væsentlige elementer i en finansiel enheds evne til at sikre overvågning af risici forbundet med tredjeparter.

(52) For at sikre, at finansielle enheder fortsat har fuld kontrol over alle udviklingstendenser, som risikerer at forringe deres IKT-sikkerhed, bør der fastsættes opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af IKT-tjenester i tilfælde af udviklingstendenser, som har en potentiel væsentlig indvirkning på evnen hos tredjepartsudbyderen af IKT-tjenester til effektivt at varetage kritiske eller vigtige funktioner, herunder levering af bistand fra sidstnævnte i tilfælde af en IKT-relateret hændelse uden yderligere omkostninger eller til en forud fastsat pris.

(53) Adgangsrettigheder samt retten til inspektion og revision, som udøves af den finansielle enhed eller en udpeget tredjepart, er afgørende instrumenter i de finansielle enheders løbende overvågning af de resultater, som tredjepartsudbyderen af IKT-tjenester opnår, kombineret med sidstnævntes fulde samarbejde i forbindelse med inspektioner. I samme ånd bør den finansielle enheds kompetente myndighed på grundlag af underretninger have adgang til at udøve den pågældende ret til at inspicere og foretage revision af tredjepartsudbyderen af IKT-tjenester, idet den er bundet af tavshedspligt.

(54) Kontraktlige ordninger bør indeholde klare opsigelsesrettigheder og dertil knyttede minimumsfrister samt særlige exitstrategier, navnlig obligatoriske overgangsperioder, i løbet af hvilke tredjepartsudbyderne af IKT-tjenester fortsat bør levere de relevante funktioner med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed eller give sidstnævnte mulighed for effektivt at skifte til andre tredjepartsudbydere af IKT-tjenester, eller alternativt at gøre brug af løsninger på stedet, der svarer overens med den leverede tjenestes kompleksitet.

(55) Desuden kan den frivillige anvendelse af de standardkontraktbestemmelser, der er udviklet af Kommissionen for cloud computing-tjenester, give de finansielle enheder og deres tredjepartsudbydere af IKT-tjenester yderligere sikkerhed ved at øge retssikkerhedsniveauet i forbindelse med den finansielle sektors anvendelse af cloud computing-tjenester, idet den fuldt ud tilpasses til de krav og forventninger, der er fastsat i forordningen om finansielle tjenesteydelser. Dette arbejde bygger på de foranstaltninger, der allerede var påtænkt i fintechhandlingsplanen fra 2018, hvori Kommissionen meddelte, at den har til hensigt at tilskynde til og fremme udarbejdelsen af standardkontraktbestemmelser for finansielle enheders anvendelse af cloud computing-tjenester, idet den trækker på indsatsen blandt tværsektorielle interessenter på området for cloud computing-tjenester, som Kommissionen har fremmet gennem inddragelse af den finansielle sektor.

(56) Med henblik på at fremme konvergens og effektivitet i forbindelse med metoder til tilsyn med IKT-tredjepartsrisici for den finansielle sektor, styrke den digitale operationelle modstandsdygtighed i finansielle enheder, der er afhængige af, at kritiske tredjepartsudbydere af IKT-tjenester varetager operationelle funktioner, og dermed bidrage til at bevare stabiliteten i EU's finansielle system og integriteten i det indre marked for finansielle tjenester, bør kritiske tredjepartsudbydere af IKT-tjenester være omfattet af en EU-tilsynsramme.

(57) Da det kun er kritiske tredjepartsudbydere, der berettiger til en særlig behandling, bør der indføres en udpegningsmekanisme med henblik på anvendelse af EU-tilsynsrammen for at tage hensyn til omfanget og karakteren af den finansielle sektors afhængighed af sådanne tredjepartsudbydere af IKT-tjenester, hvilket udmøntes i et sæt kvantitative og kvalitative kriterier, hvorved der fastsættes parametre for kritisk karakter som grundlag for medtagelse i tilsynet. Kritiske tredjepartsudbydere af IKT-tjenester, som ikke automatisk udpeges i medfør af ovennævnte kriterier, bør have mulighed for frivilligt at deltage i tilsynsrammen, mens de tredjepartsudbydere af IKT-tjenester, der allerede er omfattet af tilsynsrammer, som er fastlagt på nationalt plan med henblik på at understøtte de opgaver, der er omhandlet i artikel 127, stk. 2, i traktaten om Den Europæiske Unions funktionsmåde, derfor bør fritages.

(58) Kravet om retlig integration i EU af tredjepartsudbydere af IKT-tjenester, der er udpeget som kritiske, udgør ikke datalokalisering, da denne forordning ikke indfører yderligere krav om, at datalagring eller -behandling skal finde sted i EU.

(59) Denne ramme bør ikke berøre medlemsstaternes beføjelser til at gennemføre deres egne tilsynsmissioner i forhold til tredjepartsudbydere af IKT-tjenester, som ikke er kritiske i henhold til denne forordning, men som kan anses for at være vigtige på nationalt plan.

(60) For at løfte den nuværende institutionelle arkitektur, der består af flere lag, på området for finansielle tjenesteydelser bør Det Fælles Udvalg af ESA'er fortsat sikre den overordnede koordinering på tværs af sektorer af alle forhold, der vedrører IKT-risici, i overensstemmelse med dets opgaver vedrørende cybersikkerhed med støtte fra et nyt underudvalg ("tilsynsforummet"), der udfører det forberedende arbejde med henblik på både individuelle afgørelser rettet mod kritiske tredjepartsudbydere af IKT-tjenester og kollektive henstillinger, navnlig om benchmarking af tilsynsprogrammerne for kritiske tredjepartsudbydere af IKT-tjenester, og fastlæggelse af bedste praksis for håndtering af spørgsmål vedrørende IKT-koncentrationsrisici.

(61) For at sikre et tilsvarende tilsyn på EU-plan med tredjepartsudbydere af IKT-tjenester, der varetager en kritisk rolle i den finansielle sektors funktionsmåde, bør en af ESA'erne udpeges som ledende tilsynsførende med hver af de kritiske tredjepartsudbydere af IKT-tjenester.

(62) Ledende tilsynsførende bør have de nødvendige beføjelser til at foretage undersøgelser, inspektioner på stedet og eksterne inspektioner hos kritiske tredjepartsudbydere af IKT-tjenester, opnå adgang til alle relevante lokaler og steder og indhente fuldstændige og ajourførte oplysninger, der sætter dem i stand til at opnå en reel indsigt i typen, omfanget og virkningerne af de IKT-tredjepartsrisici, der berører de finansielle enheder og i sidste ende EU's finansielle system.

Overdragelse af hovedsvaret for tilsynet til ESA'erne udgør en forudsætning for at forstå og sætte ind over for den systemiske dimension af IKT-risici inden for finans. Det fodaftryk, som kritiske tredjepartsudbydere af IKT-tjenester efterlader i EU, og de dertil knyttede potentielle problematikker vedrørende IKT-koncentrationsrisici kræver, at der anlægges en kollektiv tilgang, som anvendes på EU-plan. Udførelsen af flere revisioner og udøvelsen af adgangsrettigheder, der gennemføres separat af en lang række kompetente myndigheder med begrænset eller ingen koordinering, vil ikke føre til et fuldstændigt tilsyn med IKT-tredjepartsrisici, samtidig med at der skabes unødvendig redundans, en unødvendig byrde og kompleksitet for kritiske tredjepartsudbydere af IKT-tjenester, der skal besvare de mange anmodninger.

(63) Desuden bør de ledende tilsynsførende kunne fremsætte henstillinger vedrørende IKT-risici og passende afhjælpende foranstaltninger, herunder gøre indsigelse mod visse kontraktlige ordninger, som i sidste ende påvirker stabiliteten i den finansielle enhed eller det finansielle system. De nationale kompetente myndigheder bør tage behørigt hensyn til efterlevelsen af sådanne væsentlige henstillinger, som er fastlagt af de ledende tilsynsførende som led i deres opgaver vedrørende tilsyn med finansielle enheder.

(64) Tilsynsrammen må hverken erstatte eller på nogen måde udskifte de finansielle enheders styring af den risiko, der er forbundet med brugen af tredjepartsudbydere af IKT-tjenester, herunder forpligtelsen til løbende at overvåge de af deres kontraktlige ordninger, der indgås med kritiske tredjepartsudbydere af IKT-tjenester, og må ikke berøre de finansielle enheders fulde ansvar for at overholde og opfylde alle krav i denne forordning og den relevante lovgivning om finansielle tjenesteydelser. For at undgå duplikationer og overlapninger bør de kompetente myndigheder afholde sig fra individuelt at træffe foranstaltninger, der har til formål at overvåge risici forbundet med den kritiske tredjepartsudbyder af IKT-tjenester. Sådanne foranstaltninger bør på forhånd koordineres og vedtages som led i tilsynsrammen.

(65) For at fremme konvergens på internationalt plan vedrørende den bedste praksis, der skal anvendes ved gennemgangen af den digitale risikostyring, der foretages af tredjepartsudbydere af IKT-tjenester, bør ESA'erne opfordres til at indgå samarbejdsordninger med de relevante kompetente tilsyns- og reguleringsmyndigheder i tredjelande for at lette udviklingen af bedste praksis vedrørende IKT-tredjepartsrisiko.

(66) Med henblik på at udnytte den tekniske ekspertise hos de kompetente myndigheders eksperter i operationel risikostyring og IKT-risikostyring bør ledende tilsynsførende trække på nationale tilsynserfaringer og oprette særlige undersøgelsesteams for hver enkelt kritisk tredjepartsudbyder af IKT-tjenester, som består af tværfaglige teams, der både støtter forberedelsen og den faktiske udførelse af tilsynsaktiviteter, herunder inspektioner på stedet hos kritiske tredjepartsudbydere af IKT-tjenester, samt den nødvendige opfølgning heraf.

(67) De kompetente myndigheder bør tillægges alle de nødvendige tilsyns-, undersøgelses- og sanktionsbeføjelser, således at de kan sikre anvendelsen af denne forordning. Administrative sanktioner bør i princippet offentliggøres. Da finansielle enheder og tredjepartsudbydere af IKT-tjenester kan have hjemsted i forskellige medlemsstater og være underlagt forskellige sektorspecifikke kompetente myndigheders tilsyn, bør der sikres tæt samarbejde mellem de relevante kompetente myndigheder, herunder ECB

for så vidt angår specifikke opgaver, som den tillægges ved Rådets forordning (EU) nr. 1024/2013[39], og høring af ESA'erne gennem gensidig informationsudveksling og levering af bistand i forbindelse med tilsynsaktiviteter.

(68) For yderligere at kvantificere og kvalificere udpegelseskriterierne for kritiske tredjepartsudbydere af IKT-tjenester og harmonisere tilsynsgebyrerne bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i traktaten om Den Europæiske Unions funktionsmåde for så vidt angår: yderligere præcisering af de systemiske virkninger, som en fejlbehæftet IKT-tredjepartstjeneste kan få for de finansielle enheder, den leverer tjenester til; antallet af globale systemisk vigtige institutter (G-SII'er) eller andre systemisk vigtige institutter (O-SII'er), som er afhængige af den pågældende tredjepartsudbyder af IKT-tjenester; antallet af tredjepartsudbydere af IKT-tjenester, der er aktive på et specifikt marked; omkostningerne forbundet med at migrere til en anden tredjepartsudbyder af IKT-tjenester; antallet af medlemsstater, hvor den pågældende tredjepartsudbyder af IKT-tjenester leverer tjenester, og hvor finansielle enheder, der benytter sig af den pågældende tredjepartsudbyder af IKT-tjenester, har aktiviteter; samt omfanget af tilsynsgebyrerne og den måde, hvorpå de skal betales.

Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning[40]. Navnlig for at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet alle dokumenter på samme tid, da medlemsstaternes eksperter og deres eksperter systematisk har adgang til møder i de af Kommissionens ekspertgrupper, som beskæftiger sig med udarbejdelsen af delegerede retsakter.

(69) Eftersom denne forordning sammen med Europa-Parlamentets og Rådets direktiv (EU) 20xx/xx[41] indebærer en konsolidering af bestemmelserne om IKT-risikostyring, der spænder over forskellige forordninger og direktiver i gældende EU-ret vedrørende finansielle tjenesteydelser, herunder forordning (EF) nr. 1060/2009, (EU) nr. 648/2012 (EU) nr. 600/2014 og (EU) nr. 909/2014, for at sikre fuld sammenhæng bør disse forordninger ændres for at præcisere, at de relevante IKT-risikorelaterede bestemmelser er fastsat i nærværende forordning.

Tekniske standarder bør sikre en konsekvent harmonisering af kravene i denne forordning. Da ESA'erne sidder inde med højt specialiseret faglig kompetence, bør de have mandat til at udarbejde udkast til reguleringsmæssige tekniske standarder, som ikke indebærer politikbeslutninger, med henblik på forelæggelse for Kommissionen. Der bør udarbejdes reguleringsmæssige tekniske standarder på områderne IKT-risikostyring, indberetning, afprøvning og centrale krav med henblik på en forsvarlig overvågning af IKT-tredjepartsrisici.

---

39 Rådets forordning (EU) nr. 1024/2013 af 15. oktober 2013 om overdragelse af specifikke opgaver til Den Europæiske Centralbank i forbindelse med politikker vedrørende tilsyn med kreditinstitutter (EUT L 287 af 29.10.2013, s. 63).

40 EUT L 123 af 12.5.2016, s. 1.

41 [*Indsæt venligst den fulde titel*].

(70) Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau. Kommissionen og ESA'erne bør sikre, at disse standarder og krav kan anvendes af alle finansielle enheder på en måde, der står i rimeligt forhold til karakteren, omfanget og kompleksiteten af disse enheder og deres aktiviteter.

(71) For at gøre det lettere at sammenligne indberetninger af større IKT-relaterede hændelser og sikre gennemsigtighed med hensyn til kontraktlige ordninger for brugen af IKT-tjenester, der leveres af tredjepartsudbydere af IKT-tjenester, bør ESA'erne have mandat til at udarbejde udkast til gennemførelsesmæssige tekniske standarder, hvorved der fastlægges standardiserede modeller, formularer og procedurer, således at finansielle enheder kan indberette IKT-relaterede hændelser, samt standardiserede modeller for registeret over oplysninger. Når ESA'erne udarbejder disse standarder, bør de tage hensyn til de finansielle enheders størrelse og kompleksitet samt karakteren af og risikoniveauet for deres aktiviteter. Kommissionen bør tillægges beføjelse til at vedtage sådanne gennemførelsesmæssige tekniske standarder ved hjælp af gennemførelsesretsakter i henhold til artikel 291 i TEUF og i overensstemmelse med artikel 15 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010. Da der allerede er fastsat yderligere krav ved delegerede retsakter og gennemførelsesretsakter baseret på de reguleringsmæssige og gennemførelsesmæssige tekniske standarder i henholdsvis forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 og (EU) nr. 909/2014, bør ESA'erne bemyndiges til enten individuelt eller i fællesskab via det fælles udvalg at forelægge reguleringsmæssige og gennemførelsesmæssige tekniske standarder for Kommissionen med henblik på vedtagelse af delegerede retsakter og gennemførelsesretsakter om overførsel og ajourføring af eksisterende regler for IKT-risikostyring.

(72) Denne vedtagelse vil medføre en efterfølgende ændring af de eksisterende delegerede retsakter og gennemførelsesretsakter, der er vedtaget på forskellige områder af lovgivningen om finansielle tjenesteydelser. Artiklerne om anvendelsesområdet for operationelle risici, i henhold til hvilke beføjelser i disse retsakter har givet mandat til vedtagelsen af delegerede retsakter og gennemførelsesretsakter, bør ændres med henblik på at overføre alle bestemmelser om digital operationel modstandsdygtighed, som i dag indgår i nævnte forordninger, til nærværende forordning.

(73) Da målene for denne forordning, navnlig om at opnå et højt niveau af digital operationel modstandsdygtighed, som omfatter alle finansielle enheder, ikke i tilstrækkelig grad kan opfyldes af medlemsstaterne, fordi de kræver harmonisering af en lang række forskellige regler, der på nuværende tidspunkt findes enten i visse EU-retsakter eller i de forskellige medlemsstaters retssystemer, men som på grund af dens omfang og virkninger bedre kan opnås på EU-plan, kan EU vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå dette mål —

VEDTAGET DENNE FORORDNING:

KAPITEL I

ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand

1. Denne forordning fastsætter følgende ensartede krav til sikkerheden i net- og informationssystemer, der understøtter de forretningsprocesser i finansielle enheder, som er nødvendige for at opnå et højt fælles niveau af digital operationel modstandsdygtighed som følger:

   a) krav til finansielle enheder vedrørende:

   – risikostyring inden for informations- og kommunikationsteknologi (IKT)

   – indberetning af større IKT-relaterede hændelser til de kompetente myndigheder

   – afprøvning af digital operationel modstandsdygtighed

   – udveksling af oplysninger og efterretninger om cybertrusler og sårbarheder

   – foranstaltninger til solid styring af IKT-tredjepartsrisici i finansielle enheder

   b) krav til de kontraktlige ordninger, der indgås mellem tredjepartsudbydere af IKT-tjenester og finansielle enheder

   c) tilsynsrammen for kritiske tredjepartsudbydere af IKT-tjenester, når de leverer tjenester til finansielle enheder

   d) regler om samarbejde mellem kompetente myndigheder og regler om de kompetente myndigheders tilsyn og håndhævelse af disse i forbindelse med alle spørgsmål, der er omfattet af denne forordning.

2. For så vidt angår finansielle enheder, der er identificeret som operatører af væsentlige tjenester i henhold til nationale bestemmelser om gennemførelse af artikel 5 i direktiv (EU) 2016/1148, betragtes denne forordning som en sektorspecifik EU-retsakt med henblik på artikel 1, stk. 7, i nævnte direktiv.

Artikel 2

Personelt anvendelsesområde

1. Denne forordning finder anvendelse på følgende enheder:

   a) kreditinstitutter

   b) betalingsinstitutter

c) e-pengeinstitutter

d) investeringsselskaber

e) udbydere af kryptoaktivtjenester, udstedere af kryptoaktiver, udstedere af aktivbaserede tokens og udstedere af signifikante aktivbaserede tokens

f) værdipapircentraler

g) centrale modparter

h) markedspladser

i) transaktionsregistre

j) forvaltere af alternative investeringsfonde

k) administrationsselskaber

l) udbydere af dataindberetningstjenester

m) forsikrings- og genforsikringsselskaber

n) forsikringsformidlere, genforsikringsformidlere og accessoriske forsikringsformidlere

o) arbejdsmarkedsrelaterede pensionskasser

p) kreditvurderingsbureauer

q) revisorer og revisionsfirmaer

r) administratorer af kritiske benchmarks

s) udbydere af crowdfundingtjenester

t) securitiseringsregistre

u) tredjepartsudbydere af IKT-tjenester.

2. Med henblik på denne forordning er den fælles benævnelse for de enheder, der er omhandlet i litra a) -t), "finansielle enheder".

Artikel 3

Definitioner

I denne forordning forstås ved:

1) "digital operationel modstandsdygtighed": en finansiel enheds evne til at opbygge, sikre og vurdere sin operationelle integritet fra et teknologisk perspektiv ved enten direkte eller indirekte og gennem anvendelse af tjenester fra en tredjepartsudbyder af IKT-tjenester at sikre det fulde spektrum af nødvendige IKT-relaterede kapaciteter med henblik på at varetage sikkerheden i de net- og informationssystemer, som en

finansiel enhed gør brug af, og som understøtter det løbende udbud af finansielle tjenesteydelser og kvaliteten heraf

2) "net- og informationssystem": et net- og informationssystem som defineret i artikel 4, nr. 1), i direktiv (EU) 2016/1148

3) "sikkerhed i net- og informationssystemer": sikkerhed i net- og informationssystemer som defineret i artikel 4, nr. 2), i direktiv (EU) 2016/1148

4) "IKT-risiko": enhver rimeligt identificerbar omstændighed i forbindelse med brugen af net- og informationssystemer — herunder funktionsfejl, kapacitetsoverskridelse, systemfejl, forstyrrelser, forringelse, fejlanvendelse, tab eller andre typer af ondsindede eller ikke-ondsindede hændelser — som, hvis de forekommer, kan kompromittere sikkerheden i net- og informationssystemerne, i eventuelle teknologiafhængige værktøjer eller processer, i den igangværende operation eller behandling eller i forbindelse med udbuddet af tjenester, og dermed kompromittere integriteten eller tilgængeligheden af data, software eller eventuelle andre komponenter, der indgår i IKT-tjenester og -infrastrukturer, eller som kan forårsage et brud på tavshedspligten, skade på fysiske IKT-infrastrukturer eller andre negative virkninger

5) "informationsaktiv": en samling af oplysninger, både materielle og immaterielle, som det er værd at beskytte

6) "IKT-relateret hændelse": en uforudset identificeret hændelse i net- og informationssystemer, hvad enten den er forårsaget af ondsindet aktivitet eller ej, som kompromitterer sikkerheden i net- og informationssystemer, i de oplysninger, som behandles, lagres eller videresendes i sådanne systemer, eller som har negative virkninger for tilgængeligheden, fortroligheden, regelmæssigheden eller autenciteten af de finansielle tjenesteydelser, som den finansielle enhed udbyder

7) "større IKT-relateret hændelse": en IKT-relateret hændelse med en potentielt stor negativ indvirkning på net- og informationssystemer, som understøtter kritiske funktioner i den finansielle enhed

8) "cybertrussel": en cybertrussel som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets forordning (EU) 2019/881[42]

9) "cyberangreb": en ondsindet IKT-relateret hændelse i form af et forsøg på ødelæggelse, eksponering, ændring, deaktivering, tyveri af eller opnåelse af uautoriseret adgang til eller uautoriseret brug af et aktiv, som forårsages af trusselsaktører

10) "trusselsefterretning": oplysninger, der er blevet sammenfattet, omdannet, analyseret, fortolket eller beriget for at skabe den rette kontekst for beslutningstagning, og som sikrer relevant og tilstrækkelig forståelse med henblik på at afbøde virkningerne af

[42] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).

en IKT-relateret hændelse eller cybertrussel, herunder de tekniske detaljer ved et cyberangreb, kendskab til dem, der er ansvarlige for angrebet, deres måde at operere på og deres hensigter

11) "forsvar i dybden": en IKT-relateret strategi, der involverer mennesker, processer og teknologi, og som skal indføre forskellige barrierer på tværs af flere lag og dimensioner i enheden

12) "sårbarhed": en svaghed, følsomhed eller fejl i forbindelse med et aktiv, et system, en proces eller en kontrolfunktion, som kan udnyttes af en trussel

13) "trusselsbaseret penetrationstest": en ramme, der efterligner de taktikker, teknikker og procedurer, som bruges af rigtige trusselsaktører og betragtes som reelle cybertrusler, og som muliggør en kontrolleret, skræddersyet, efterretningsbaseret (rødt team) test af enhedens kritiske live-produktionssystemer

14) "IKT-tredjepartsrisiko": en IKT-risiko, der kan opstå for en finansiel enhed i forbindelse med dens brug af IKT-tjenester, der leveres af tredjepartsudbydere af IKT-tjenester eller af sidstnævntes øvrige underleverandører

15) "tredjepartsudbyder af IKT-tjenester": en virksomhed, der leverer digitale tjenester og datatjenester, herunder udbydere af cloud computing-tjenester, software, datanalysetjenester, datacentre, men eksklusive udbydere af hardwarekomponenter og virksomheder, som er meddelt tilladelse i henhold til EU-ret, og som leverer elektroniske kommunikationstjenester, jf. definitionen i artikel 2, nr. 4), i Europa-Parlamentets og Rådets direktiv (EU) 2018/1972[43]

16) "IKT-tjenester": digitale tjenester og datatjenester, der leveres gennem IKT-systemer til én eller flere interne eller eksterne brugere, herunder levering af datatjenester, dataindlæsnings-, datalagrings-, databehandlings- og -indberetningstjenester, dataovervågningstjenester samt databaserede forretningstjenester og beslutningsstøttetjenester

17) "kritisk eller vigtig funktion": en funktion, som, hvis dens gennemførelse afbrydes, er fejlbehæftet eller mislykkes, i væsentlig grad kan forringe en finansiel enheds opfyldelse af de betingelser og forpligtelser, der er forbundet med dens tilladelse, eller af dens andre forpligtelser i henhold til gældende lovgivning om finansielle tjenesteydelser, eller forringe dens finansielle resultater, soliditeten eller kontinuiteten af dens tjenester og aktiviteter

18) "kritisk tredjepartsudbyder af IKT-tjenester": en tredjepartsudbyder af IKT-tjenester, der er udpeget i overensstemmelse med artikel 29 og omfattet af den i artikel 30-37 omhandlede tilsynsramme

19) "tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland": en tredjepartsudbyder af IKT-tjenester, som er en juridisk person med hjemsted i et tredjeland, som ikke har etableret en virksomhed/er tilstede i Unionen, og som har indgået kontraktlige ordninger med en finansiel enhed om levering af IKT-tjenester

[43] Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning) (EUT L 321 af 17.12.2018, s. 36).

20) "IKT-underleverandør med hjemsted i et tredjeland": en IKT-underleverandør, som er en juridisk person med hjemsted i et tredjeland, som ikke har etableret en virksomhed/er tilstede i Unionen, og som har indgået kontraktlige ordninger enten med en tredjepartsudbyder af IKT-tjenester eller med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland

21) "IKT-koncentrationsrisiko": eksponering for individuelle eller flere indbyrdes forbundne kritiske tredjepartsudbydere af IKT-tjenester, som skaber en grad af afhængighed af sådanne udbydere, der bevirker, at manglende tilgængelighed, fejl eller andre typer af mangler i forbindelse med sidstnævnte potentielt kan være til fare for en finansiel enheds evne, og i sidste ende Unionens finansielle system som helhed, til at varetage kritiske funktioner eller håndtere andre former for negative virkninger, herunder store tab

22) "ledelsesorgan": et ledelsesorgan, jf. definitionen i artikel 4, stk. 1, nr. 36), i direktiv 2014/65/EU, artikel 3, stk. 1, nr. 7, i direktiv 2013/36/EU, artikel 2, stk. 1, litra s), i direktiv 2009/65/EF, artikel 2, stk. 1, nr. 45), i Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014, artikel 3, stk. 1, nr. 20, i forordning (EU) 2016/1011[44], artikel 3, stk. 1, litra u), i Europa-Parlamentets og Rådets forordning (EU) 20xx/xx [MiCA][45], eller dertil svarende personer, som varetager den faktiske drift af enheden eller nøglefunktioner i overensstemmelse med relevant EU-lovgivning eller national lovgivning

23) "kreditinstitut": et kreditinstitut som defineret i artikel 4, stk. 1, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013[46]

24) "investeringsselskab": et investeringsselskab som defineret i artikel 4, stk. 1, nr. 1), i direktiv 2014/65/EU

25) "betalingsinstitut": et betalingsinstitut som defineret i artikel 1, stk. 1, litra d), i direktiv (EU) 2015/2366

26) "e-pengeinstitut": et e-pengeinstitut som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets direktiv 2009/110/EF[47]

27) "central modpart": en central modpart som defineret i artikel 2, nr. 1), i forordning (EU) nr. 648/2012

28) "transaktionsregister": et transaktionsregister som defineret i artikel 2, nr. 2), i forordning (EU) nr. 648/2012

---

44 Europa-Parlamentets og Rådets forordning (EU) 2016/1011 af 8. juni 2016 om indeks, der bruges som benchmarks i finansielle instrumenter og finansielle kontrakter eller med henblik på at måle investeringsfondes økonomiske resultater, og om ændring af direktiv 2008/48/EF og 2014/17/EU samt forordning (EU) nr. 596/2014 (EUT L 171 af 29.6.2016, s. 1).

45 [*indsæt venligst den fulde titel og EUT-henvisning*].

46 Europa-parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber og om ændring af forordning (EU) nr. 648/2012 (EUT L 176 af 27.6.2013, s. 1).

47 Europa-Parlamentets og Rådets direktiv 2009/110/EF af 16. september 2009 om adgang til at optage og udøve virksomhed som udsteder af elektroniske penge og tilsyn med en sådan virksomhed, ændring af direktiv 2005/60/EF og 2006/48/EF og ophævelse af direktiv 2000/46/EF (EUT L 267 af 10.10.2009, s. 7).

29) "værdipapircentral": en værdipapircentral som defineret i artikel 2, stk. 1, nr. 1), i forordning (EU) nr. 909/2014

30) "markedsplads": en markedsplads som defineret i artikel 4, stk. 1, nr. 24), i direktiv 2014/65/EU

31) "forvalter af alternative investeringsfonde": en forvalter af alternative investeringsfonde som defineret i artikel 4, stk. 1, litra b),i direktiv 2011/61/EU

32) "administrationsselskab": et administrationsselskab som defineret i artikel 2, stk. 1, litra b), i direktiv 2009/65/EF.

33) "udbyder af dataindberetningstjenester": en udbyder af dataindberetningstjenester som defineret i artikel 4, stk. 1, nr. 63), i direktiv 2014/65/EU

34) "forsikringsselskab": et forsikringsselskab som defineret i artikel 13, nr. 1), i direktiv 2009/138/EF

35) "genforsikringsselskab": et genforsikringsselskab som defineret i artikel 13, nr. 4), i direktiv 2009/138/EF

36) "forsikringsformidler: en forsikringsformidler som defineret i artikel 2, stk. 1, nr. 3), i direktiv (EU) 2016/97

37) "accessorisk forsikringsformidler": en accessorisk forsikringsformidler som defineret i artikel 2, stk. 1, nr. 4), i direktiv (EU) 2016/97

38) "genforsikringsformidler: en genforsikringsformidler som defineret i artikel 2, stk. 1, nr. 5), i direktiv (EU) 2016/97

39) "arbejdsmarkedsrelateret pensionskasse": en arbejdsmarkedsrelateret pensionskasse som defineret i artikel 6, nr. 1, i direktiv (EU) 2016/2341

40) "kreditvurderingsbureau": et kreditvurderingsbureau som defineret i artikel 3, stk. 1, litra b), i forordning (EF) nr. 1060/2009

41) "revisor": en revisor som defineret i artikel 2, nr. 2), i direktiv 2006/43/EF

42) "revisionsfirma": et revisionsfirma som defineret i artikel 2, nr. 3), i direktiv 2006/43/EF

43) "udbyder af kryptoaktivtjenester": en udbyder af kryptoaktivtjenester som defineret i artikel 3, stk. 1, litra n), i forordning (EU) 202x/xx [*Publikationskontor: Indsæt venligst henvisning til MiCA-forordningen*];

44) "udsteder af kryptoaktiver": en udsteder af kryptoaktiver som defineret i artikel 3, stk. 1, litra h), i [*EUT: Indsæt venligst henvisning til MiCA-forordningen*]

45) "udsteder af aktivbaserede tokens": en udsteder af aktivbaserede betalingstokens som defineret i artikel 3, stk. 1, litra i), [*EUT: Indsæt venligst henvisning til MiCA-forordningen*];

46) "udsteder af signifikante aktivbaserede tokens": en udsteder af signifikante aktivbaserede betalingstokens som defineret i artikel 3, stk. 1, litra j), i [*EUT: Indsæt venligst henvisning til MiCA-forordningen*];

47) "administrator af kritiske benchmarks": en administrator af kritiske benchmarks som defineret i artikel x, litra x), i forordning 202x/xx [*EUT: Indsæt venligst henvisning til MiCA-forordningen*]

48) "udbyder af crowdfundingtjenester": en udbyder af crowdfundingtjenester som defineret i artikel x, litra x), i forordning (EU) 202x/xx [*Publikationskontor: Indsæt venligst henvisning til MiCA-forordningen*];

49) "securitiseringsregister": et securitiseringsregister som defineret i artikel 2, nr. 23), i forordning (EU) 2017/2402

50) "mikrovirksomhed": en finansiel enhed som defineret i artikel 2, stk. 3, i bilaget til henstilling 2003/361/EF.

KAPITEL II

IKT-RISIKOSTYRING

AFDELING I

Artikel 4

Styring og organisation

1. Finansielle enheder skal have indført interne styrings- og kontrolrammer, der sikrer en effektiv og forsigtig styring af alle IKT-risici.

2. Ledelsesorganet i den finansielle enhed fastlægger, godkender, fører tilsyn med og har ansvar for gennemførelsen af alle ordninger vedrørende de rammer for IKT-risikostyring, der er omhandlet i artikel 5, stk. 1.

   Med henblik på første afsnit er det ledelsesorganet, som

   a) påtager sig det endelige ansvar for styringen af den finansielle enheds IKT-risici

   b) fastlægger klare roller og ansvarsområder for alle IKT-relaterede funktioner

   c) fastsætter en passende risikotolerancetærskel for IKT-risici i den pågældende finansielle enhed, jf. artikel 5, stk. 9, litra b)

   d) godkender, fører tilsyn med og regelmæssigt gennemgår gennemførelsen af den finansielle enheds politik for IKT-driftsstabilitet og IKT-katastrofeberedskabsplan, jf. henholdsvis artikel 10, stk. 1 og 3

e) godkender og regelmæssigt gennemgår IKT-revisionsplaner, IKT-revisioner og væsentlige ændringer heraf

f) tildeler og regelmæssigt gennemgår et passende budget for at opfylde den finansielle enheds behov i forbindelse med digital operationel modstandsdygtighed med hensyn til alle ressourcetyper, herunder kurser i IKT-risici og -færdigheder for alt relevant personale

g) godkender og regelmæssigt gennemgår den finansielle enheds politik vedrørende ordninger for brug af IKT-tjenester, der leveres af tredjepartsudbydere af IKT-tjenester

h) behørigt underrettes om de ordninger, der er indgået med tredjepartsudbydere af IKT-tjenester vedrørende brugen af IKT-tjenester, om relevante planlagte væsentlige ændringer, som vedrører tredjepartsudbydere af IKT-tjenester, og om potentielle virkninger af sådanne ændringer på de kritiske eller vigtige funktioner, der er omfattet af disse ordninger, herunder modtagelse af en sammenfatning af risikoanalysen med henblik på at vurdere virkningerne af disse ændringer

i) behørigt underrettes om IKT-relaterede hændelser og deres virkninger samt om indsatsforanstaltninger, genopretningsforanstaltninger og korrigerende foranstaltninger.

3. Finansielle enheder, som ikke er mikrovirksomheder, skal oprette en overvågningsrolle for de ordninger, der er indgået med tredjepartsudbydere af IKT-tjenester, vedrørende brugen af IKT-tjenester, eller udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation.

4. Medlemmerne af ledelsesorganet deltager regelmæssigt i særlige kurser for at opnå tilstrækkelig viden og tilstrækkelige færdigheder og ajourføre disse, således at de kan forstå og vurdere IKT-risici og deres virkninger for den finansielle enheds transaktioner.

AFDELING II

Artikel 5

Ramme for IKT-risikostyring

1. Finansielle enheder indfører en forsvarlig, udførlig og veldokumenteret ramme for IKT-risikostyring, der sætter dem i stand til at håndtere IKT-risikoen på hurtig, effektiv og fyldestgørende vis, og sikrer et højt niveau af digital operationel modstandsdygtighed, som matcher deres forretningsmæssige behov, størrelse og kompleksitet.

2. Den i stk. 1 omhandlede ramme for IKT-risikostyring skal omfatte strategier, politikker, procedurer, IKT-protokoller og -værktøjer, som er nødvendige for på behørig og effektiv vis at beskytte alle relevante fysiske komponenter og

infrastrukturer, herunder computerhardware, servere samt alle relevante lokaler, datacentre og sensitive udpegede områder, for at sikre tilstrækkelig beskyttelse af alle disse fysiske elementer mod risici, herunder skade og uautoriseret adgang eller brug.

3. De finansielle enheder minimerer virkningerne af IKT-risici ved at indføre passende strategier, politikker, procedurer, protokoller og værktøjer som fastsat i rammen for IKT-risikostyring. De forelægger fuldstændige og ajourførte oplysninger om IKT-risici som krævet af de kompetente myndigheder.

4. Som led i den stk. 1 omhandlede ramme for IKT-risikostyring gennemfører finansielle enheder, som ikke er mikrovirksomheder, et system til styring af informationssikkerhed, som er baseret på anerkendte internationale standarder og er i overensstemmelse med tilsynsmæssige retningslinjer, og reviderer det regelmæssigt.

5. Finansielle enheder, som ikke er mikrovirksomheder, sikrer en passende adskillelse af IKT-styringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

6. Den stk. 1 omhandlede ramme for IKT-risikostyring skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større IKT-hændelser, og i henhold til tilsynsmæssige instrukser eller konklusioner, som er udledt af relevant afprøvning af digital operationel modstandsdygtighed eller revisionsprocesser. Den skal forbedres løbende på grundlag af indhøstede gennemførelses- og overvågningserfaringer.

7. Den stk. 1 omhandlede ramme for IKT-risikostyring gennemgås regelmæssigt af IKT-revisorer, der besidder tilstrækkelig viden, faglig kompetence og ekspertise med hensyn til IKT-risici. IKT-revisioners hyppighed og fokus skal stå i rimeligt forhold til den finansielle enheds IKT-risici.

8. Der fastlægges en formel opfølgningsproces, herunder regler for rettidig efterprøvning og udbedring af kritiske resultater af IKT-revisioner, idet der tages højde for konklusionerne fra revisionsgennemgangen og hensyn til karakteren, omfanget og kompleksiteten af de finansielle enheders tjenester og aktiviteter.

9. Den stk. 1 omhandlede ramme for IKT-risikostyring skal omfatte en strategi for digital modstandsdygtighed, der fastsætter, hvordan rammen gennemføres. Med henblik herpå skal den omfatte metoderne til håndtering af IKT-risici og opfylde specifikke IKT-mål ved at

   a) redegøre for, hvordan rammen for IKT-risikostyring understøtter den finansielle enheds forretningsstrategi og -mål

   b) fastlægge risikotolerancetærsklen for IKT-risici i overensstemmelse med den finansielle enheds risikovillighed og analysere tolerancen over for virkninger af IKT-forstyrrelser

   c) fastsætte klare informationssikkerhedsmål

   d) redegøre for IKT-referencearkitekturen og eventuelle ændringer, der er nødvendige for at nå specifikke forretningsmål

e) beskrive de forskellige indførte mekanismer til detektion, beskyttelse og forebyggelse af virkningerne af IKT-relaterede hændelser

f) dokumentere antallet af indberettede større IKT-relaterede hændelser og forebyggende foranstaltningers effektivitet

g) fastlægge en holistisk strategi på enhedsplan med flere IKT-udbydere, som viser, hvor der er stor afhængighed af tredjepartsudbydere af IKT-tjenester, og anføre begrundelsen for denne udbudssammensætning bestående af tredjepartsudbydere af IKT-tjenester

h) gennemføre afprøvning af digital operationel modstandsdygtighed

i) indeholde en kommunikationsstrategi, der anvendes i tilfælde af IKT-relaterede hændelser.

10. Efter godkendelse fra de kompetente myndigheder kan finansielle enheder uddelegere de opgaver, der er forbundet med efterprøvning af overholdelsen af kravene til IKT-risikostyring, til koncerninterne eller eksterne virksomheder.

Artikel 6

IKT-systemer, -protokoller og-værktøjer

1. De finansielle enheder anvender og vedligeholder opdaterede IKT-systemer, -protokoller og -værktøjer, som opfylder følgende betingelser:

a) Systemerne og værktøjerne er velegnede i forhold til karakteren, arten, kompleksiteten og omfanget af de transaktioner, der ligger til grund for deres aktiviteter.

b) De er pålidelige.

c) De besidder tilstrækkelig kapacitet til med nøjagtighed at behandle de data, der er nødvendige for udførelsen af aktiviteterne og rettidig levering af tjenesterne, og til at håndtere spidsbelastninger, ordre- og meddelelsesmængder eller transaktionsmængder efter behov, herunder når der indføres ny teknologi.

d) De er teknologisk modstandsdygtige nok til i tilstrækkeligt omfang at håndtere yderligere behov for informationsbehandling som krævet under stressede markedsforhold eller i andre vanskelige situationer.

2. Hvis finansielle enheder anvender internationalt anerkendte tekniske standarder og sektorens førende praksis for informationssikkerhed og interne IKT-kontroller, anvender de disse standarder og fremgangsmåder i overensstemmelse med eventuelle relevante tilsynsmæssige henstillinger vedrørende inkorporering heraf.

Artikel 7

Identifikation

1. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 5, stk. 1, varetager de finansielle enheder identifikation, klassificering og tilstrækkelig dokumentering af alle IKT-relaterede forretningsfunktioner, de informationsaktiver, der understøtter disse funktioner, samt IKT-systemets konfigurationer og sammenkoblinger med interne og eksterne IKT-systemer. De finansielle enheder vurderer efter behov og mindst én gang om året, hvorvidt klassificeringen af informationsaktiverne er tilstrækkelig, og eventuel relevant dokumentation.

2. De finansielle enheder identificerer løbende alle kilder til IKT-risici, navnlig risikoeksponeringen for og fra andre finansielle enheder, og vurderer cybertrusler og IKT-sårbarheder, der er relevante for deres IKT-relaterede forretningsfunktioner og informationsaktiver. De finansielle enheder gennemgår regelmæssigt og mindst én gang om året de risikoscenarier, der har virkninger for dem.

3. Finansielle enheder, som ikke er mikrovirksomheder, foretager en risikovurdering, hver gang der foretages en større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker deres funktioner, hjælpeprocesser eller informationsaktiver.

4. De finansielle enheder identificerer alle IKT-systemkonti, herunder konti på eksterne steder, netressourcerne og hardwareudstyret, og kortlægger det fysiske udstyr, der anses for kritisk. De kortlægger IKT-aktivernes konfiguration samt forbindelserne og den indbyrdes forbundethed mellem de forskellige IKT-aktiver.

5. De finansielle enheder identificerer og dokumenterer alle processer, der er afhængige af tredjepartsudbydere af IKT-tjenester, og identificerer sammenkoblinger med tredjepartsudbydere af IKT-tjenester.

6. Med henblik på stk. 1, 4 og 5 opretholder finansielle enheder relevante fortegnelser og ajourfører dem regelmæssigt.

7. Finansielle enheder, som ikke er mikrovirksomheder, foretager regelmæssigt og mindst én gang om året en specifik IKT-risikovurdering af alle nedarvede IKT-systemer, navnlig før og efter sammenkobling af gamle og nye teknologier, applikationer eller systemer.

Artikel 8

Beskyttelse og forebyggelse

1. Med henblik på at sikre passende beskyttelse af IKT-systemer og tilrettelægge indsatsforanstaltninger sikrer de finansielle enheder løbende overvågning af og kontrol med, hvordan IKT-systemerne og -værktøjerne fungerer, og minimerer virkningerne af sådanne risici ved at indføre passende IKT-sikkerhedsværktøjer, -politikker og -procedurer.

2. De finansielle enheder udformer, indkøber og gennemfører IKT-sikkerhedsstrategier, -politikker, -procedurer, -protokoller og -værktøjer, der navnlig har til formål at sikre IKT-systemernes modstandsdygtighed, stabilitet og tilgængelighed og opretholde høje standarder for datasikkerhed, datafortrolighed og -integritet, hvad enten dataene er inaktive, i brug eller under overførsel.

3. For at nå de i stk. 2 omhandlede mål anvender de finansielle enheder den mest avancerede IKT-teknologi og de mest avancerede IKT-processer, som

   a) garanterer sikkerheden for metoderne til overførsel af oplysninger

   b) minimerer risikoen for korruption eller tab af data, uautoriseret adgang og tekniske fejl, der kan hæmme erhvervsaktiviteten

   c) forhindrer lækage af oplysninger

   d) sikrer, at data beskyttes mod dårlig administration eller procesrelaterede risici, herunder utilstrækkelig registreringspraksis.

4. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 5, stk. 1, skal de finansielle enheder

   (a) udvikle og dokumentere en informationssikkerhedspolitik, der fastlægger regler for beskyttelse af fortroligheden, integriteten og tilgængeligheden af deres egne og deres kunders IKT-ressourcer, data og informationsaktiver

   b) følge en risikobaseret tilgang, indføre en forsvarlig forvaltning af netværk og infrastrukturer ved anvendelse af passende teknikker, metoder og protokoller, herunder gennemføre automatiske mekanismer til isolering af de berørte informationsaktiver i tilfælde af cyberangreb

   c) gennemføre politikker, der begrænser den fysiske og virtuelle adgang til IKT-systemressourcer og -data udelukkende til det, der er påkrævet for legitime og godkendte funktioner og aktiviteter, og med henblik herpå indføre en række politikker, procedurer og kontroller vedrørende adgangsrettigheder og en forsvarlig forvaltning heraf

   d) gennemføre politikker og protokoller for stærke autentificeringsmekanismer på grundlag af relevante standarder og særlige kontrolsystemer, som skal forhindre adgang til krypteringsnøgler, hvorigennem data krypteres baseret på resultaterne fra godkendte klassificerings- og risikovurderingsprocesser

   e) gennemføre politikker, procedurer og kontroller for styring af IKT-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsændringer, som er baseret på en risikovurderingstilgang, og som en integreret del af den finansielle enheds overordnede ændringsstyringsproces, for at sikre, at alle ændringer af IKT-systemer registreres, afprøves, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde

   f) sørge for, at der indføres passende og udførlige politikker for programrettelser og opdateringer.

Med henblik på litra b) udformer de finansielle enheder infrastrukturen for netværkstilslutning på en sådan måde, at den kan afbrydes øjeblikkeligt, og sikrer, at den adskilles og segmenteres for at minimere og forhindre afsmitning, navnlig i forbindelse med indbyrdes forbundne finansielle processer.

Med henblik på litra e) skal IKT-ændringsstyringsprocessen godkendes på passende ledelsesniveauer og omfatte specifikke protokoller, der gør det muligt at foretage hasteændringer.

Artikel 9

Detektion

1. De finansielle enheder indfører mekanismer til omgående detektion af anormale aktiviteter i overensstemmelse med artikel 15, herunder problemer med IKT-netværkets ydeevne og IKT-relaterede hændelser, og til identifikation af alle potentielt væsentlige lokale fejl (single points of failure).

   De i første afsnit omhandlede mekanismer afprøves regelmæssigt i overensstemmelse med artikel 22.

2. Ved de i stk. 1 omhandlede detektionsmekanismer skal det gøres muligt at anvende flere kontrollag, fastlægge varslingstærskler og -kriterier, som skal udløse detektion af IKT-relaterede hændelser og indsatsforanstaltninger mod IKT-relaterede hændelser, og indføre automatiske varlingsmekanismer for det relevante personale, som har ansvar for indsatsen mod IKT-relaterede hændelser.

3. Under behørig hensyntagen til deres størrelse, forretnings- og risikoprofiler, afsætter finansielle enheder tilstrækkelige ressourcer og kapaciteter til overvågning af brugeraktiviteter, forekomsten af IKT-anomalier og IKT-relaterede hændelser, navnlig cyberangreb.

4. Finansielle enheder som omhandlet i artikel 2, stk. 1, litra l), indfører desuden systemer, som effektivt kan kontrollere, om handelsindberetningerne er fuldstændige, identificere udeladelser og åbenbare fejl og anmode om fornyet fremsendelse af enhver således fejlbehæftet indberetning.

Artikel 10

Indsats og genopretning

1. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 5, stk. 1, og baseret på de krav til identifikation, der er fastsat i artikel 7, indfører de finansielle enheder en målrettet og udførlig politik for IKT-driftsstabilitet som en integreret del af den finansielle enheds politik for operationel driftsstabilitet.

2. De finansielle enheder gennemfører den i stk. 1 omhandlede politik for IKT-driftsstabilitet ved hjælp af målrettede, passende og veldokumenterede ordninger, planer, procedurer og mekanismer, der tager sigte mod:

a) at indberette alle IKT-relaterede hændelser

b) at sikre, at den finansielle enheds kritiske funktioner er stabile

c) hurtigt, passende og effektivt at sætte ind over for og løse alle IKT-relaterede hændelser, navnlig, men ikke udelukkende, cyberangreb, på en måde, der begrænser skaden og prioriterer genoptagelsen af aktiviteter og genopretningstiltag

d) omgående at aktivere målrettede planer, der gør det muligt at anvende inddæmningsforanstaltninger, -processer og -teknologier, der er velegnede til de enkelte typer IKT-relaterede hændelser, og som forhindrer yderligere skade, samt skræddersyede indsats- og genopretningsprocedurer, der er fastlagt i henhold til artikel 11

e) at anslå foreløbige virkninger, skader og tab

f) at indføre kommunikations- og krisestyringstiltag, der sikrer, at ajourførte oplysninger videresendes til al relevant internt personale og eksterne interessenter i overensstemmelse med artikel 13, og at de indberettes til de kompetente myndigheder i overensstemmelse med artikel 17.

3. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 5, stk. 1, gennemfører de finansielle enheder en dertil knyttet IKT-katastrofeberedskabsplan, som for finansielle enheder, der ikke er mikrovirksomheder, underkastes uafhængige revisionsgennemgange.

4. De finansielle enheder indfører, vedligeholder og foretager regelmæssig afprøvning af passende planer for IKT-driftsstabilitet, navnlig med hensyn til kritiske eller vigtige funktioner, som outsources eller udliciteres gennem ordninger, der er indgået med tredjepartsudbydere af IKT-tjenester.

5. Som led i deres samlede IKT-risikostyring skal de finansielle enheder

a) afprøve deres politik for IKT-driftsstabilitet og IKT-katastrofeberedskabsplan mindst én gang om året og efter væsentlige ændringer af IKT-systemerne

b) afprøve de krisekommunikationsplaner, der er udarbejdet i henhold til artikel 13.

Med henblik på litra a) medtager finansielle enheder, som ikke er mikrovirksomheder, sikkerhedskopier og de overflødige faciliteter, der er nødvendige for at opfylde de i artikel 11 fastsatte forpligtelser, i afprøvningsplanerne for cyberangrebscenarier og omstillingsscenarier mellem den primære IKT-infrastruktur og redundante kapacitet.

De finansielle enheder gennemgår regelmæssigt deres politik for IKT-driftsstabilitet og IKT-katastrofeberedskabsplan under hensyntagen til resultaterne af test, der er gennemført i overensstemmelse med første afsnit, og henstillinger, der bygger på revisionskontrol eller tilsynsmæssige gennemgange.

6. Finansielle enheder, som ikke er mikrovirksomheder, har en krisestyringsfunktion, som, hvis deres politik for IKT-driftsstabilitet og IKT-katastrofeberedskabsplan aktiveres, skal indeholde klare procedurer for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 13.

7. De finansielle enheder fører registre over aktiviteter før og under driftsforstyrrelser, når deres IKT-driftsstabilitet og IKT-katastrofeberedskabsplan aktiveres. Sådanne registre skal være let tilgængelige.

8. Finansielle enheder som omhandlet i artikel 2, stk. 1, litra f), forelægger kopier af resultaterne af de test af IKT-driftsstabiliteten eller lignende aktiviteter, der gennemføres i den relevante periode, for de kompetente myndigheder.

9. Finansielle enheder, som ikke er mikrovirksomheder, indberetter alle omkostninger og tab, der opstår som følge af IKT-relaterede forstyrrelser og hændelser, til de kompetente myndigheder.

Artikel 11

Politikker for sikkerhedskopiering og genopretningsmetoder

1. Med henblik på at sikre genopretning af IKT-systemer med minimal nedetid og begrænsede forstyrrelser udvikler de finansielle enheder som led i deres ramme for IKT-risikostyring følgende:

   a) en politik for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller sensitive karakter

   b) genopretningsmetoder.

2. Systemer til sikkerhedskopiering bør uden unødigt ophold påbegynde behandlingen, medmindre en sådan påbegyndelse sætter sikkerheden i net- og informationssystemer, dataintegriteten eller -fortroligheden over styr.

3. Når de finansielle enheder genopretter sikkerhedskopierede data ved anvendelse af egne systemer, anvender de IKT-systemer, der har et andet operativmiljø end hovedmiljøet, og som ikke er direkte forbundet med sidstnævnte og er sikkert beskyttet mod uautoriseret adgang eller IKT-korruption.

   For finansielle enheder som omhandlet i artikel 2, stk. 1, litra g), skal genopretningsplaner gøre det muligt at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, således at den berørte centrale modpart kan opretholde driftssikkerheden og gennemføre afviklingen på den planlagte dato.

4. De finansielle enheder opretholder redundante IKT-kapaciteter, der er udstyret med ressourcer og funktionaliteter, der er tilstrækkelige og passende med henblik på at sikre forretningsmæssige behov.

5. Finansielle enheder som omhandlet i artikel 2, stk. 1, litra f), opretholder eller sikrer, at deres tredjepartsudbydere af IKT-tjenester bibeholder mindst ét sekundært

afviklingssted, der er udstyret med ressourcer, kapaciteter, funktionaliteter og personalemæssige ordninger, der er tilstrækkelige og velegnede til at sikre forretningsmæssige behov.

Det sekundære afviklingssted skal

a) befinde sig i en geografisk afstand fra det primære afviklingssted for at sikre, at det har en særlig risikoprofil og for at forhindre, at det påvirkes af den hændelse, der har berørt det primære afviklingssted

b) kunne sikre driftsstabiliteten for kritiske tjenester på samme måde som det primære afviklingssted eller levere det serviceniveau, der er nødvendigt for, at den finansielle enhed kan udføre sine kritiske transaktioner inden for rammerne af genopretningsmålene

c) være umiddelbart tilgængeligt for den finansielle enheds personale for at sikre driftsstabilitet for kritiske tjenester, hvis det primære afviklingssted er blevet utilgængeligt.

6. Når de finansielle enheder fastlægger målene for genopretningstid og -punkt for hver funktion, tager de hensyn til de potentielle overordnede virkninger for markedseffektiviteten. Sådanne tidsmål skal sikre, at de aftalte serviceniveauer overholdes i ekstreme scenarier.

7. Når de finansielle enheder foretager genopretning efter en IKT-relateret hændelse, udfører de flere kontroller, herunder afstemninger, for at sikre, at dataintegriteten er af højeste standard. Disse kontroller foretages også i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er enslydende.

Artikel 12

Læring og udvikling

1. De finansielle enheder sørger for at råde over kapaciteter og personale, alt efter deres størrelse, forretnings- og risikoprofiler, som kan indsamle oplysninger om sårbarheder og cybertrusler, IKT-relaterede hændelser, navnlig cyberangreb, og analysere deres sandsynlige virkninger for deres digitale operationelle modstandsdygtighed.

2. De finansielle enheder foretager gennemgange af IKT-relaterede hændelser efter væsentlige IKT-forstyrrelser, som berører deres kerneaktiviteter, analyserer årsagerne til forstyrrelserne og identificerer nødvendige forbedringer af IKT-operationerne eller inden for rammerne af den i artikel 10 omhandlede politik for IKT-driftsstabilitet.

Når finansielle enheder, som ikke er mikrovirksomheder, gennemfører ændringer, underrettes de kompetente myndigheder om disse ændringer.

I forbindelse med de i første afsnit omhandlede gennemgange af IKT-relaterede hændelser skal det fastslås, om de fastlagte procedurer blev fulgt, og om de iværksatte foranstaltninger var effektive, herunder i forhold til følgende:

a) den hastighed, med hvilken der blev sat ind over for sikkerhedsvarsler og virkningerne af IKT-relaterede hændelser og deres omfang blev fastslået

b) kvaliteten og hastigheden af udførelsen af den kriminaltekniske analyse

c) effektiviteten af den finansielle enheds fejlafhjælpning i forbindelse med hændelser

d) effektiviteten af den interne og eksterne kommunikation.

3. Erfaringer fra afprøvning af digital operationel modstandsdygtighed, som foretages i overensstemmelse med artikel 23 og 24, og fra faktiske IKT-relaterede hændelser, navnlig cyberangreb, samt udfordringer i forbindelse med aktiveringen af planer for driftsstabilitet eller genopretningsplaner skal sammen med relevante oplysninger, der udveksles med modparter, og som vurderes i forbindelse med tilsynsmæssige gennemgange, løbende integreres i IKT-risikovurderingsprocessen. Disse resultater skal udmøntes i passende gennemgange af relevante komponenter i den ramme for IKT-risikostyring, der er omhandlet i artikel 5, stk. 1.

4. De finansielle enheder overvåger effektiviteten af gennemførelsen af deres strategi for digital modstandsdygtighed, jf. artikel 5, stk. 9. De kortlægger udviklingen i IKT-risici over tid, analyserer hyppigheden, typerne, omfanget af og udviklingen i IKT-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed, med henblik på at forstå graden af IKT-risikoeksponering og forbedre den finansielle enheds cybermodenhed og cyberberedskab.

5. Højtstående IKT-personale skal mindst én gang om året aflægge rapport til ledelsesorganet om de i stk. 3 omhandlede resultater og fremsætte anbefalinger.

6. De finansielle enheder udvikler programmer til bevidstgørelse om IKT-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelsesordninger. Disse skal omfatte alle medarbejdere og den øverste ledelse.

De finansielle enheder overvåger løbende den relevante teknologiske udvikling også med henblik på at forstå mulige virkninger af indførelsen af sådanne nye teknologier for kravene til IKT-sikkerhed og digital operationel modstandsdygtighed. De skal holde sig ajour med de seneste IKT-risikostyringsprocesser og effektivt imødegå aktuelle eller nye former for cyberangreb.

Artikel 13
Kommunikation

1. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 5, stk. 1, sørger de finansielle enheder for at indføre kommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af IKT-relaterede hændelser eller væsentlige

sårbarheder for kunder og modparter samt for offentligheden, alt efter hvad der er relevant.

2. Som led i den ramme for IKT-risikostyring, der er omhandlet i artikel 5, stk. 1, gennemfører de finansielle enheder kommunikationsplaner for personalet og for eksterne interessenter. Kommunikationspolitikkerne for personalet skal tage hensyn til behovet for at skelne mellem personale, der er involveret i IKT-risikostyring, navnlig indsats og genopretning, og personale, der skal underrettes.

3. Mindst én person i enheden skal have til opgave at gennemføre kommunikationsstrategien for IKT-relaterede hændelser og til dette formål varetage rollen som talsperson for offentligheden og medierne.

Artikel 14

Yderligere harmonisering af IKT-risikostyringsværktøjer, -metoder, -processer og -politikker

Den Europæiske Banktilsynsmyndighed (EBA), Den Europæiske Værdipapir- og Markedstilsynsmyndighed (ESMA) og Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger (EIOPA) udarbejder i samråd med Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) udkast til reguleringsmæssige tekniske standarder med følgende formål:

a) at præcisere, hvilke yderligere elementer der skal indgå i de IKT-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er omhandlet i artikel 8, stk. 2, med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier mod indtrængen og datamisbrug, bevare dataenes ægthed og integritet, herunder kryptografiske teknikker, og garantere en nøjagtig og hurtig dataoverførsel uden større forstyrrelser

b) at foreskrive, hvordan de IKT-sikkerhedspolitikker, -procedurer og -værktøjer, der er omhandlet i artikel 8, stk. 2, skal omfatte sikkerhedskontroller i systemerne fra begyndelsen (indbygget sikkerhed), give mulighed for tilpasninger til et trusselsbillede i udvikling og sørge for, at der bruges teknologi til sikring af forsvar i dybden

c) yderligere at præcisere de relevante teknikker, metoder og protokoller, der er omhandlet i artikel 8, stk. 4, litra b)

d) at videreudvikle komponenter i kontrollen med de rettigheder vedrørende adgangsforvaltning, der er omhandlet i artikel 8, stk. 4, litra c), og den dertil knyttede HR-politik med angivelse af adgangsrettigheder, procedurer for tildeling og tilbagekaldelse af rettigheder, overvågning af anormal adfærd i forbindelse med IKT-risici ved hjælp af passende indikatorer, herunder for mønstre vedrørende netværksbrug, tidspunkter, IT-aktivitet og ukendt udstyr

e) at videreudvikle de elementer, der er anført i artikel 9, stk. 1, og som muliggør en hurtig detektion af anormale aktiviteter, og de kriterier, der er omhandlet i artikel 9, stk. 2, og som udløser detektion af IKT-relaterede hændelser og indsatsforanstaltninger

f) yderligere at præcisere de komponenter, der er indeholdt den politik for IKT-driftsstabilitet, der er omhandlet i artikel 10, stk. 1

g) yderligere at præcisere afprøvningen af de planer for IKT-driftsstabilitet, der er omhandlet i artikel 10, stk. 5, for at sikre, at der tages behørigt hensyn til de scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes, og at der tages behørigt hensyn til de potentielle virkninger af insolvens hos eller andre fejl forårsaget af eventuelle relevante tredjepartsudbydere af IKT-tjenester og, hvor det er relevant, de politiske risici i de respektive udbyderes jurisdiktioner

h) yderligere at præcisere de komponenter, der er indeholdt i den politik for IKT-katastrofeberedskabsplan, der er omhandlet i artikel 10, stk. 3.

EBA, ESMA og EIOPA forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den [*Publikationskontoret: Indsæt datoen 1 år efter ikrafttrædelsesdatoen*].

Kommissionen tillægges beføjelse til at vedtage de i første afsnit omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

KAPITEL III

IKT-RELATEREDE HÆNDELSER

STYRING, KLASSIFICERING OG INDBERETNING

Artikel 15

Proces for styring af IKT-relaterede hændelser

1. De finansielle enheder fastlægger og gennemfører en proces for styring af IKT-relaterede hændelser for at detektere, styre og indberette IKT-relaterede hændelser og indfører tidlige advarselsindikatorer som varslinger.

2. De finansielle enheder fastlægger passende procedurer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af IKT-relaterede hændelser, således at de grundlæggende årsager identificeres og udryddes for at forhindre, at sådanne hændelser forekommer.

3. I henhold til den proces for styring af IKT-relaterede hændelser, der er omhandlet i stk. 1,

   a) skal der fastlægges procedurer til at identificere, spore, kategorisere og klassificere IKT-relaterede hændelser alt efter deres prioritet og de berørte tjenesters størrelse og kritiske betydning i overensstemmelse med de kriterier, der er omhandlet i artikel 16, stk. 1

b) skal der tildeles roller og ansvarsområder, som skal aktiveres for forskellige IKT-relaterede hændelsestyper og -scenarier

c) skal der udarbejdes planer for kommunikation til personale, eksterne interessenter og medier i overensstemmelse med artikel 13 og for underretning af kunder, interne fejlafhjælpningsprocedurer, herunder IKT-relaterede kundeklager, samt for indgivelse af oplysninger til finansielle enheder, der fungerer som modparter, alt efter hvad der er relevant

d) skal det sikres, at større IKT-relaterede hændelser indberettes til den relevante øverste ledelse, at ledelsesorganet underrettes om større IKT-relaterede hændelser, og der skal redegøres for virkningerne, indsatsen og yderligere kontroller, som skal indføres som følge af IKT-relaterede hændelser

e) skal der træffes indsatsforanstaltninger mod IKT-relaterede hændelser, som skal afbøde virkningerne og sikre, at tjenesterne bliver operationelle og sikre på en rettidig måde.

Artikel 16

Klassificering af IKT-relaterede hændelser

1. De finansielle enheder klassificerer IKT-relaterede hændelser og fastslår deres virkninger på grundlag af følgende kriterier:

a) antallet af brugere eller finansielle modparter, som er berørt af den forstyrrelse, der er forårsaget af den IKT-relaterede hændelse, og hvorvidt den IKT-relaterede hændelse har haft indvirkning på omdømmet

b) varigheden af den IKT-relaterede hændelse, herunder tjenestens nedetid

c) den geografiske udbredelse med hensyn til de områder, der er berørt af den IKT-relaterede hændelse, navnlig hvis den berører mere end to medlemsstater

d) de datatab, som den IKT-relaterede hændelse medfører, såsom tab af integritet, tab af fortrolighed eller tab af tilgængelighed

e) omfanget af den IKT-relaterede hændelses virkninger for den finansielle enheds IKT-systemer

f) den kritiske betydning af de berørte tjenester, herunder den finansielle enheds transaktioner og operationer

g) de økonomiske virkninger af den IKT-relaterede hændelse i både absolutte og relative tal.

2. ESA'erne udarbejder via Det Fælles Udvalg af ESA'er ("det fælles udvalg") og efter høring af Den Europæiske Centralbank (ECB) og ENISA et fælles udkast til reguleringsmæssige tekniske standarder, som yderligere præciserer følgende:

a) kriterierne i stk. 1, herunder væsentlighedstærskler til bestemmelse af større IKT-relaterede hændelser, som er omfattet af indberetningspligten i artikel 17, stk. 1

b) de kriterier, som de kompetente myndigheder skal anvende med henblik på at vurdere større IKT-relaterede hændelsers relevans for andre medlemsstaters jurisdiktioner, og nærmere oplysninger om IKT-relaterede hændelser, som skal udveksles med andre kompetente myndigheder i henhold til artikel 17, stk. 5 og 6.

3. Når ESA'erne udarbejder de i stk. 2 omhandlede fælles udkast til reguleringsmæssige tekniske standarder, tager de hensyn til internationale standarder samt de specifikationer, der er udarbejdet og offentliggjort af ENISA, herunder, hvor det er relevant, specifikationer for andre økonomiske sektorer.

ESA'erne forelægger disse fælles udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den [*Publikationskontoret: Indsæt datoen 1 år efter ikrafttrædelsesdatoen*].

Kommissionen tillægges beføjelse til supplere denne forordning ved at vedtage de i stk. 2 omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikel 17

Indberetning af større IKT-relaterede hændelser

1. Definansielle enheder indberetter større IKT-relaterede hændelser til den relevante kompetente myndighed som omhandlet i artikel 41 inden for de frister, der er fastsat i stk. 3.

Med henblik på første afsnit udarbejder de finansielle enheder efter indsamling og analyse af alle relevante oplysninger en indberetning om hændelser ved anvendelse af den model, der er omhandlet i artikel 18, og indgiver den til den kompetente myndighed.

Indberetningen skal indeholde alle de oplysninger, der er nødvendige for, at den kompetente myndighed kan fastslå, hvorvidt den større IKT-relaterede hændelse er væsentlig, og vurdere mulige grænseoverskridende virkninger.

2. Hvis en større IKT-relateret hændelse har eller kan få virkninger for tjenestebrugeres og kunders finansielle interesser, underretter de finansielle enheder uden unødigt ophold deres tjenestebrugere og kunder om den større IKT-relaterede hændelse og underretter dem så hurtigt som muligt om alle de foranstaltninger, der er truffet for at afbøde de negative virkninger af en sådan hændelse.

3. De finansielle enheder indgiver følgende til den kompetente myndighed som omhandlet i artikel 41:

a) en indledende underretning, uden ophold og senest ved forretningsdagens afslutning, eller, hvis der er tale om en større IKT-relateret hændelse, som fandt sted senere end 2 timer inden forretningsdagens afslutning, senest 4 timer efter begyndelsen af den næste forretningsdag eller, hvis der ikke findes indberetningskanaler, så snart de bliver tilgængelige

b) en foreløbig rapport senest 1 uge efter den indledende underretning, jf. litra a), efterfulgt af ajourførte underretninger, hver gang der foreligger en relevant ajourføring af status, samt efter en specifik anmodning fra den kompetente myndighed

c) en endelig rapport, når den grundlæggende årsagsanalyse er afsluttet, uanset om der allerede er gennemført afbødende foranstaltninger eller ej, og når tallene for de faktiske virkninger foreligger med henblik på at erstatte skøn, dog senest en måned fra det tidspunkt, hvor den første indberetning indgives.

4. De finansielle enheder må kun uddelegere indberetningsforpligtelserne i henhold til denne artikel til en tredjepartsudbyder af tjenester, hvis den relevante kompetente myndighed har godkendt uddelegeringen, jf. artikel 41.

5. Når den kompetente myndighed modtager den i stk. 1 omhandlede rapport, forelægger den kompetente myndighed uden unødigt ophold nærmere oplysninger om hændelsen for:

a) EBA, ESMA eller EIOPA, alt efter hvad der er relevant

b) ECB, alt efter hvad der er relevant, i tilfælde af finansielle enheder som omhandlet i artikel 2, stk. 1, litra a)–c) og

c) det centrale kontaktpunkt, der er udpeget i henhold til artikel 8 i direktiv (EU) 2016/1148.

6. EBA, ESMA eller EIOPA og ECB vurderer relevansen af den større IKT-relaterede hændelse for andre relevante offentlige myndigheder og underretter dem så hurtigt som muligt herom. ECB underretter medlemmerne af Det Europæiske System af Centralbanker om spørgsmål, der er relevante for betalingssystemet. De kompetente myndigheder træffer på grundlag af underretningen, hvis det er hensigtsmæssigt, alle nødvendige foranstaltninger for at beskytte det finansielle systems umiddelbare stabilitet.

Artikel 18

Harmonisering af indholdet af og modeller for indberetninger

1. ESA'erne udarbejder via det fælles udvalg og efter høring af ENISA og ECB følgende:

a) fælles udkast til reguleringsmæssige tekniske standarder med henblik på:

1) at fastlægge indholdet af indberetninger om større IKT-relaterede hændelser

2) yderligere at præcisere betingelserne for finansielle enheders uddelegering af de indberetningsforpligtelser, der er fastsat i dette kapitel, til en tredjepartsudbyder af tjenester efter forudgående godkendelse fra den kompetente myndighed

b) fælles udkast til gennemførelsesmæssige tekniske standarder for at fastlægge standardformularer, -modeller og -procedurer, som de finansielle enheder skal bruge ved indberetning af en større IKT-relateret hændelse.

ESA'erne forelægger det fælles udkast til reguleringsmæssige tekniske standarder, der er omhandlet i stk. 1, litra a), og det fælles udkast til gennemførelsesmæssige tekniske standarder, der er omhandlet i stk. 1, litra b), for Kommissionen senest den xx 202x [*Publikationskontoret: Indsæt datoen 1 år efter ikrafttrædelsesdatoen*].

Kommissionen tillægges beføjelse til supplere denne forordning ved at vedtage de fælles reguleringsmæssige tekniske standarder, der er omhandlet i stk. 1, litra a), i overensstemmelse med artikel 10-14 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1095/2010 og (EU) nr. 1094/2010.

Kommissionen tillægges beføjelse til at vedtage de fælles gennemførelsesmæssige tekniske standarder, der er omhandlet i stk. 1, litra b), i overensstemmelse med artikel 15 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1095/2010 og (EU) nr. 1094/2010.

Artikel 19

Centralisering af indberetninger af større IKT-relaterede hændelser

1. ESA'erne udarbejder via det fælles udvalg og i samråd med ECB og ENISA en fælles rapport med en vurdering af muligheden for yderligere centralisering af indberetningen af hændelser gennem oprettelse af et fælles EU-knudepunkt for finansielle enheders indberetning af større IKT-relaterede hændelser. I rapporten skal det undersøges, hvordan man kan fremme strømmen af indberetninger af IKT-relaterede hændelser, reducere de dermed forbundne omkostninger og understøtte tematiske analyser med henblik på at øge den tilsynsmæssige konvergens.

2. Den i stk. 1 omhandlede rapport skal mindst omfatte følgende elementer:

a) forudsætninger for oprettelsen af et sådant EU-knudepunkt

b) fordele, begrænsninger og mulige risici

c) elementer af den operationelle styring

d) betingelser for medlemskab

e) vilkår for finansielle enheders og nationale kompetente myndigheders adgang til EU-knudepunktet

f) en foreløbig vurdering af de finansielle omkostninger, der er forbundet med oprettelsen af en operationel platform, der understøtter EU-knudepunktet, herunder den nødvendige ekspertise

3. ESA'erne forelægger den i stk. 1 omhandlede rapport for Kommissionen, Europa-Parlamentet og Rådet senest den xx 202x [*EUT: Indsæt datoen 3 år efter ikrafttrædelsesdatoen*].

Artikel 20

Tilsynsmæssig feedback

1. Når den kompetente myndighed modtager en indberetning som omhandlet i artikel 17, stk. 1, kvitterer den for modtagelsen af underretningen og giver hurtigst muligt den finansielle enhed alle nødvendige tilbagemeldinger eller retningslinjer, navnlig for at drøfte afhjælpende foranstaltninger på enhedsplan eller måder, hvorpå negative virkninger kan minimeres på tværs af sektorer.

2. ESA'erne aflægger via det fælles udvalg en årlig rapport baseret på et anonymiseret og samlet grundlag for underretninger om IKT-relaterede hændelser, der er modtaget fra kompetente myndigheder, der som minimum angiver antallet af større IKT-relaterede hændelser, deres karakter, virkninger for finansielle enheders eller kunders transaktioner, omkostninger og de afhjælpende foranstaltninger, der er truffet.

ESA'erne udsteder advarsler og udarbejder statistikker på højt niveau for at understøtte IKT-trussels- og sårbarhedsvurderinger.

KAPITEL IV

AFPRØVNING AF DIGITAL OPERATIONEL MODSTANDSDYGTIGHED

Artikel 21

Generelle krav til gennemførelsen af afprøvning af digital operationel modstandsdygtighed

1. Med henblik på at vurdere beredskabet i forhold til IKT-relaterede hændelser, identificere svagheder, mangler eller huller i den digitale operationelle modstandsdygtighed og straks træffe korrigerende foranstaltninger udarbejder, opretholder og ajourfører de finansielle enheder under behørig hensyntagen til deres størrelse, forretnings- og risikoprofiler et forsvarligt og udførligt program for afprøvning af digital operationel modstandsdygtighed som en integrerende del af den i artikel 5 omhandlede ramme for IKT-risikostyring.

2. Programmet for afprøvning af den digitale operationelle modstandsdygtighed skal omfatte en række vurderinger, test, metodologier, fremgangsmåder og værktøjer, der skal anvendes i overensstemmelse med bestemmelserne i artikel 22 og 23.

3. Når de finansielle enheder gennemfører det i stk. 1 omhandlede program for afprøvning af den digitale operationelle modstandsdygtighed, følger de en risikobaseret tilgang, idet de tager hensyn til et IKT-risikomiljø i udvikling, eventuelle specifikke risici, som den finansielle enhed udsættes for eller kan blive udsat for, informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre forhold, som den finansielle enhed finder relevante.

4. De finansielle enheder sikrer, at afprøvninger gennemføres af uafhængige parter, hvad enten de er interne eller eksterne.

5. De finansielle enheder fastlægger procedurer og politikker med henblik på at prioritere, klassificere og afhjælpe alle problemer, der anerkendes i forbindelse med gennemførelsen af test, og fastlægger interne valideringsmetoder for at sikre, at alle konstaterede svagheder, mangler eller huller afhjælpes fuldt ud.

6. De finansielle enheder tester alle kritiske IKT-systemer og -applikationer mindst én gang om året.

Artikel 22

Afprøvning af IKT-værktøjer og -systemer

1. Det i artikel 21 omhandlede program for afprøvning af den digitale operationelle modstandsdygtighed skal indeholde bestemmelser om gennemførelse af en komplet vifte af relevante test, herunder sårbarhedsvurderinger og -scanninger, analyser af open source software, vurderinger af netsikkerheden, analyser af huller, fysiske sikkerhedsgennemgange, spørgeskemaer og løsninger til scanningssoftware, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest, end-to-end-test eller penetrationstest.

2. Finansielle enheder som omhandlet i artikel 2, stk. 1, litra f) og g), foretager sårbarhedsvurderinger inden indførelse eller genindførelse af nye eller eksisterende tjenester, der understøtter den finansielle enheds kritiske funktioner, applikationer og infrastrukturkomponenter.

Artikel 23

Avanceret afprøvning af IKT-værktøjer, -systemer og -processer ud fra trusselsbaserede penetrationstest

1. Finansielle enheder, der er identificeret i overensstemmelse med stk. 4, foretager mindst hvert 3. år avancerede test ved hjælp af trusselsbaserede penetrationstest.

2. Trusselsbaserede penetrationstest skal som minimum omfatte en finansiel enheds kritiske funktioner og tjenester og foretages på live-produktionssystemer, der understøtter sådanne funktioner. Det nøjagtige omfang af trusselsbaserede penetrationstest, der baseres på en vurdering af kritiske funktioner og tjenester, fastsættes af de finansielle enheder og valideres af de kompetente myndigheder.

Med henblik på første afsnit identificerer de finansielle enheder alle relevante underliggende IKT-processer, -systemer og -teknologier, der understøtter kritiske funktioner og tjenester, herunder funktioner og tjenester, der outsources eller udliciteres til tredjepartsudbydere af IKT-tjenester.

Hvis tredjepartsudbydere af IKT-tjenester medtages i den trusselsbaserede penetrationstest, træffer den finansielle enhed de nødvendige foranstaltninger til at sikre disse udbyderes deltagelse.

De finansielle enheder anvender effektiv risikostyringskontrol for at mindske risici for potentielle virkninger for data, skade på aktiver og forstyrrelser for kritiske tjenester eller transaktioner i den finansielle enhed selv, hos dens modparter eller i den finansielle sektor.

Efter afslutning af testen, og efter at der er opnået enighed om rapporter og udbedringsplaner, forelægger den finansielle enhed og de eksterne testere den kompetente myndighed dokumentation, som bekræfter, at den trusselsbaserede penetrationstest er blevet gennemført i overensstemmelse med kravene. De kompetente myndigheder validerer dokumentationen og udsteder en erklæring.

3. De finansielle enheder kontakter testere i overensstemmelse med artikel 24 med henblik på at gennemføre trusselsbaserede penetrationstest.

De kompetente myndigheder identificerer finansielle enheder med henblik på at gennemføre trusselsbaserede penetrationstest på en måde, der er forholdsmæssigt afpasset til den finansielle enheds størrelse, omfang, aktivitet og overordnede risikoprofil, på grundlag af en vurdering af følgende:

a) virkningsrelaterede faktorer, navnlig den kritiske betydning af de tjenester, der leveres, og de aktiviteter, der udføres af den finansielle enhed

b) eventuelle betænkeligheder vedrørende finansiel stabilitet, herunder den finansielle enheds systemiske karakter på nationalt plan eller på EU-plan, alt efter hvad der er relevant

c) den finansielle enheds specifikke IKT-risikoprofil, grad af IKT-modenhed eller de teknologiske kendetegn, der er involveret.

4. EBA, ESMA og EIOPA udarbejder efter høring af ECB og under hensyntagen til de relevante EU-rammer, som finder anvendelse på efterretningsbaserede penetrationstest, udkast til reguleringsmæssige tekniske standarder med henblik på yderligere at præcisere følgende:

a) de kriterier, der anvendes med henblik på anvendelsen af stk. 3

b) kravene vedrørende

a) omfanget af de i stk. 2 omhandlede trusselsbaserede penetrationstest

b) den testmetode og -tilgang, der skal følges for hver specifik fase af testprocessen

c) resultaterne af testen, testens afslutnings- og udbedringsfaser

c) den type tilsynsmæssigt samarbejde, der er nødvendigt for at gennemføre trusselsbaserede penetrationstest i forbindelse med finansielle enheder, der opererer i mere end én medlemsstat, således at der sikres et passende niveau af tilsynsmæssig deltagelse og en fleksibel gennemførelse for at tage højde for særlige forhold i de finansielle delsektorer eller lokale finansielle markeder.

ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den [*EUT: Indsæt datoen 2 måneder forud for ikrafttrædelsesdatoen*].

Kommissionen tillægges beføjelse til supplere denne forordning ved at vedtage de i andet afsnit omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1095/2010 og (EU) nr. 1094/2010.

Artikel 24

Krav til testere

1. De finansielle enheder må kun anvende testere til udrulning af trusselsbaserede penetrationstest, som

   a) er de mest egnede, og som har det bedste omdømme

   b) er i besiddelse af tekniske og organisatoriske kapaciteter og har specifik ekspertise med hensyn til trusselsefterretning, penetrationstest eller red team-test

   c) er certificerede af et akkrediteringsorgan i en medlemsstat eller overholder formelle adfærdskodekser eller etiske rammer

   d) hvis der er tale om eksterne testere, giver på uafhængig vis sikkerhed eller en revisionspåtegning vedrørende forsvarlig risikostyring, som vedrører gennemførelsen af trusselsbaserede penetrationstest, herunder behørig beskyttelse af den finansielle enheds fortrolige oplysninger og afhjælpning af den finansielle enheds forretningsrisici

   e) hvis der er tale om eksterne testere, er behørigt og fuldt ud dækket af relevante erhvervsansvarsforsikringer, herunder mod risici for forseelser og forsømmelighed.

2. De finansielle enheder sikrer, at der i de aftaler, der er indgået med eksterne testere, kræves en forsvarlig forvaltning af resultaterne af den trusselsbaserede penetrationstest, og at enhver behandling heraf, herunder enhver form for generering, udkast, lagring, aggregering, rapportering, kommunikation eller destruktion, ikke medfører risici for den finansielle enhed.

KAPITEL V

STYRING AF IKT-TREDJEPARTSRISICI

AFDELING I

NØGLEPRINCIPPER FOR FORSVARLIG STYRING AF IKT-TREDJEPARTSRISICI

Artikel 25

Generelle principper

De finansielle enheder styrer IKT-tredjepartsrisici som en integreret del af IKT-risici inden for deres ramme for IKT-risikostyring og i overensstemmelse med følgende principper:

1. Finansielle enheder, der har indgået kontraktlige ordninger for brugen af IKT-tjenester til drift af deres forretningsaktiviteter, har til enhver tid det fulde ansvar for at overholde og opfylde alle forpligtelser i henhold til denne forordning og gældende lovgivning om finansielle tjenesteydelser.

2. De finansielle enheders styring af IKT-tredjepartsrisici skal gennemføres i overensstemmelse med proportionalitetsprincippet, idet der tages hensyn til følgende:

   a) omfang, kompleksitet og betydning af den IKT-relaterede afhængighed

   b) de risici, der opstår som følge af kontraktlige ordninger for brugen af IKT-tjenester, der er indgået med tredjepartsudbydere af IKT-tjenester, under hensyntagen til den kritiske betydning eller vigtighed af den pågældende tjeneste, proces eller funktion og til de potentielle virkninger for driftsstabiliteten og kvaliteten af finansielle tjenesteydelser og aktiviteter på individuelt plan og koncernniveau.

3. De finansielle enheder vedtager og gennemgår regelmæssigt en strategi for IKT-tredjepartsrisici som led i deres ramme for IKT-risikostyring, idet de tager hensyn til den strategi med flere udbydere, der er omhandlet i artikel 5, stk. 9, litra g). Denne strategi skal omfatte en politik for brugen af IKT-tjenester, der leveres af tredjepartsudbydere af IKT-tjenester, og skal gælde på individuelt grundlag og, alt efter hvad der er relevant, på delkonsolideret og konsolideret grundlag. Ledelsesorganet gennemgår regelmæssigt de risici, der er konstateret i forbindelse med outsourcing af kritiske eller vigtige funktioner.

4. Som led i deres ramme for IKT-risikostyring opretholder og ajourfører de finansielle enheder på delkonsolideret og konsolideret niveau et register over oplysninger om alle kontraktlige ordninger for brugen af IKT-tjenester, der leveres af tredjepartsudbydere af IKT-tjenester.

De i første afsnit omhandlede kontraktlige ordninger skal være behørigt dokumenteret, idet der skelnes mellem dem, der dækker kritiske eller vigtige funktioner, og dem, der ikke gør.

De finansielle enheder indberetter mindst én gang om året oplysninger til de kompetente myndigheder om antallet af nye ordninger om brugen af IKT-tjenester, kategorierne af tredjepartsudbydere af IKT-tjenester, typen af kontraktlige ordninger og de tjenester og funktioner, der leveres.

De finansielle enheder stiller efter anmodning det fulde register over oplysninger eller, som anmodet, nærmere angivne afsnit heraf til rådighed for den kompetente myndighed sammen med eventuelle oplysninger, som anses for nødvendige for at muliggøre et effektivt tilsyn med den finansielle enhed.

De finansielle enheder underretter rettidigt den kompetente myndighed om planlagt udlicitering af kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

5. Inden de finansielle enheder indgår en kontraktlig ordning om brugen af IKT-tjenester, skal de

   a) vurdere, om den kontraktlige ordning omfatter en kritisk eller vigtig funktion

   b) vurdere, om de tilsynsmæssige betingelser for udlicitering er opfyldt

   c) identificere og vurdere alle relevante risici i forbindelse med den kontraktlige ordning, herunder muligheden for, at sådanne kontraktlige ordninger kan bidrage til at øge IKT-koncentrationsrisikoen

   d) udvise al mulig rettidig omhu over for potentielle tredjepartsudbydere af IKT-tjenester og under alle udvælgelses- og vurderingsprocesserne sikre, at den pågældende tredjepartsudbyder af IKT-tjenester er velegnet

   e) identificere og vurdere interessekonflikter, som de kontraktlige ordninger kan give anledning til.

6. De finansielle enheder må kun indgå kontraktlige ordninger med tredjepartsudbydere af IKT-tjenester, der overholder høje, passende og de seneste standarder for informationssikkerhed.

7. Når finansielle enheder udøver adgangs-, inspektions- og revisionsrettigheder over for tredjepartsudbyderen af IKT-tjenester, foretager de ud fra en risikobaseret tilgang en forudgående fastsættelse af hyppigheden af revisioner og inspektioner og de områder, der skal underkastes revision, idet de overholder almindeligt accepterede revisionsstandarder i overensstemmelse med eventuelle tilsynsmæssige instrukser vedrørende anvendelse og inkorporering af sådanne revisionsstandarder.

   Med hensyn til kontraktlige ordninger, der indebærer en høj grad af teknologisk kompleksitet, efterprøver den finansielle enhed, om revisorer, hvad enten de interne revisorer, puljer af revisorer eller eksterne revisorer, besidder de nødvendige færdigheder og den nødvendige viden til effektivt at udføre relevante revisioner og vurderinger.

8. De finansielle enheder skal sikre, at de kontraktlige ordninger for brugen af IKT-tjenester som minimum opsiges under følgende omstændigheder:

a) overtrædelser begået af tredjepartsudbyderen af IKT-tjenester af gældende love, administrative bestemmelser eller brud på kontraktvilkår

b) forhold, der er identificeret under overvågningen af IKT-tredjepartsrisici, og som anses for at kunne ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af IKT-tjenester

c) svagheder hos tredjepartsudbyderen af IKT-tjenester, som er påvist i dennes overordnede IKT-risikostyring, og navnlig i den måde, hvorpå denne garanterer sikkerheden og integriteten af fortrolige, personlige eller på anden måde sensitive oplysninger eller andre oplysninger end personoplysninger

d) omstændigheder, hvor den kompetente myndighed ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af de respektive kontraktlige ordninger.

9. De finansielle enheder indfører exitstrategier for at tage højde for de risici, der kan opstå hos tredjepartsudbyderen af IKT-tjenester, navnlig muligheden for, at sidstnævnte går fallit, en forringelse af kvaliteten af de leverede funktioner, eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller mangelfuld levering af tjenester eller væsentlige risici i forhold til en passende og løbende anvendelse af funktionen.

De finansielle enheder sikrer, at de kan opsige kontraktlige ordninger, uden

a) at deres forretningsaktiviteter afbrydes

b) at efterlevelsen af de forskriftsmæssige krav begrænses

c) at kontinuiteten og kvaliteten af deres levering af tjenester til kunder lider skade.

Exitstrategierne skal være udførlige, veldokumenterede og, hvor det er relevant, afprøvet i tilstrækkeligt omfang.

De finansielle enheder identificerer alternative løsninger og udarbejder overgangsplaner, således at de kan fratage tredjepartsudbyderen af IKT-tjenester de udliciterede funktioner og de relevante data og foretage en sikker og integreret overførsel af disse til alternative udbydere eller på ny inkorporere dem internt.

De finansielle enheder træffer passende beredskabsforanstaltninger for at opretholde driftsstabiliteten under alle de i første afsnit omhandlede omstændigheder.

10. ESA'erne udarbejder via det fælles udvalg udkast til gennemførelsesmæssige tekniske standarder for at fastlægge standardmodeller med henblik på det i stk. 4 omhandlede register over oplysninger.

ESA'erne forelægger disse udkast til gennemførelsesmæssige tekniske standarder for Kommissionen senest den [*EUT: Indsæt datoen 1 år efter denne forordnings ikrafttrædelsesdato*].

Kommissionen tillægges beføjelse til at vedtage de i første afsnit omhandlede gennemførelsesmæssige tekniske standarder i overensstemmelse med artikel 15 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1095/2010 og (EU) nr. 1094/2010.

11. ESA'erne udarbejder via det fælles udvalg udkast til reguleringsmæssige standarder

a) for yderligere at præcisere det detaljerede indhold af den i stk. 3 omhandlede politik vedrørende de kontraktlige ordninger for brugen af IKT-tjenester, som leveres af tredjepartsudbydere af IKT-tjenester, idet der henvises til de vigtigste faser i livscyklussen for de respektive ordninger for brugen af IKT-tjenester

b) for de typer af oplysninger, der skal indgå i det i stk. 4 omhandlede register over oplysninger.

ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den [*Publikationskontoret: Indsæt datoen 1 år efter ikrafttrædelsesdatoen*].

Kommissionen tillægges beføjelse til supplere denne forordning ved at vedtage de i andet afsnit omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1095/2010 og (EU) nr. 1094/2010.

Artikel 26

Foreløbig vurdering af IKT-koncentrationsrisiko og yderligere ordninger for videreoutsourcing

1. Når finansielle enheder foretager identifikation og vurdering af IKT-koncentrationsrisici som omhandlet i artikel 25, stk. 5, litra c), tager de hensyn til, hvorvidt indgåelsen af en kontraktlig ordning i forbindelse med IKT-tjenester vil føre til et af følgende forhold:

a) udlicitering til en tredjepartsudbyder af IKT-tjenester, som ikke er let at erstatte, eller

b) der er indgået flere kontraktlige ordninger om levering af IKT-tjenester med den samme tredjepartsudbyder af IKT-tjenester eller med tredjepartsudbydere af IKT-tjenester, som har tætte forbindelser til denne.

De finansielle enheder afvejer fordelene og omkostningerne ved alternative løsninger, såsom brugen af forskellige tredjepartsudbydere af IKT-tjenester, under hensyntagen til, hvorvidt og hvordan de påtænkte løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i deres strategi for digital modstandsdygtighed.

2. Hvis den kontraktlige ordning for brugen af IKT-tjenester omfatter muligheden for, at en tredjepartsudbyder af IKT-tjenester yderligere giver en kritisk eller vigtig funktion i underentreprise til andre tredjepartsudbydere af IKT-tjenester, afvejer de finansielle enheder de fordele og risici, der kan opstå i forbindelse med en sådan underentreprise, navnlig hvis der er tale om en IKT-underleverandør med hjemsted i et tredjeland.

Hvis der er indgået kontraktlige ordninger for brugen af IKT-tjenester med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland, betragter de finansielle enheder mindst følgende faktorer for relevante:

a) overholdelsen af databeskyttelse

b) effektiv håndhævelse af lovgivningen

c) bestemmelser om insolvens, som finder anvendelse, hvis tredjepartsudbyderen af IKT-tjenester går konkurs

d) eventuelle begrænsninger, der kan opstå i forbindelse med en hastende genopretning af den finansielle enheds data.

'De finansielle enheder vurderer, hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at overvåge de udliciterede funktioner og den kompetente myndigheds evne til i denne henseende at føre effektivt tilsyn med den finansielle enhed.

Artikel 27

De vigtigste kontraktbestemmelser

1. Rettigheder og forpligtelser for den finansielle enhed og for tredjepartsudbyderen af IKT-tjenester skal fordeles klart og fastlægges skriftligt. Den samlede kontrakt, som omfatter serviceniveauaftaler, skal dokumenteres i et skriftligt dokument, som parterne har adgang til på papir eller i et tilgængeligt format, som kan downloades.

2. De kontraktlige ordninger for brugen af IKT-tjenester skal mindst omfatte følgende:

a) en klar og fuldstændig beskrivelse af alle funktioner og tjenester, som tredjepartsudbyderen af IKT-tjenester skal levere, med angivelse af, om underentreprise af en kritisk eller vigtig funktion eller væsentlige dele heraf er tilladt, og i bekræftende fald de betingelser, der gælder for en sådan underentreprise

b) de steder, hvor de udliciterede funktioner og tjenester eller funktionerne og tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og kravet om, at tredjepartsudbyderen af IKT-tjenester skal underrette den finansielle enhed, hvis den har planer om at ændre sådanne steder

c) bestemmelser om adgang til, tilgængelighed, integritet, sikkerhed og beskyttelse af personoplysninger og om sikring af adgang, genopretning og

tilbagesendelse i et let tilgængeligt format af personoplysninger og andre data end personoplysninger, der behandles af den finansielle enhed, i tilfælde af insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen af IKT-tjenester varetager

d) en fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og gennemgange heraf, og præcise kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, således at den finansielle enhed kan foretage en effektiv overvågning, og således at der uden unødigt ophold kan træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes

e) opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af IKT-tjenester over for den finansielle enhed, herunder underretning om enhver udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen af IKT-tjenester har evnen til effektivt at udføre kritiske eller vigtige funktioner i overensstemmelse med aftalte serviceniveauer

f) forpligtelsen for tredjepartsudbyderen af IKT-tjenester til at yde bistand i tilfælde af en IKT-hændelse, uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd

g) krav til tredjepartsudbyderen af IKT-tjenester om at gennemføre og teste beredskabsplaner og indføre IKT-sikkerhedsforanstaltninger, -værktøjer og -politikker, som i tilstrækkelig grad garanterer, at den finansielle enhed kan foretage en sikker levering af tjenester i overensstemmelse med dens lovramme

h) retten til løbende at overvåge det præstationsniveau, som tredjepartsudbyderen af IKT-tjenester leverer, og som omfatter følgende:

   i) den finansielle enheds eller en udpeget tredjeparts ret til adgang, inspektion og revision samt retten til at tage kopier af relevant dokumentation, hvis faktiske udøvelse ikke hindres eller begrænses af andre kontraktlige ordninger eller gennemførelsespolitikker

   ii) retten til at nå til enighed om alternative sikkerhedsniveauer, hvis andre kunders rettigheder påvirkes

   iii) forpligtelsen til fuldt ud at samarbejde under de inspektioner på stedet, som den finansielle enhed udfører, og nærmere oplysninger om omfanget af, vilkårene for og hyppigheden af revisioner fra fjernt hold

i) forpligtelsen for tredjepartsudbyderen af IKT-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, herunder personer, som de har udpeget

j) opsigelsesrettigheder og dertil knyttede minimumsfrister for opsigelse af kontrakten i overensstemmelse med de kompetente myndigheders forventninger

k) exitstrategier, navnlig indførelse af en obligatorisk passende overgangsperiode:

a) i løbet af hvilken tredjepartsudbyderen af IKT-tjenester fortsat leverer de respektive funktioner eller tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed

b) som giver den finansielle enhed mulighed for at skifte til en anden tredjepartsudbyder af IKT-tjenester eller skifte til løsninger på stedet, der svarer overens med den leverede tjenestes kompleksitet.

3. Når finansielle enheder og tredjepartsudbydere af IKT-tjenester forhandler om kontraktlige ordninger, overvejer de anvendelsen af standardkontraktbestemmelser, der er udviklet til specifikke tjenester.

4. ESA'erne udarbejder via det fælles udvalg udkast til reguleringsmæssige tekniske standarder med henblik på yderligere at præcisere de elementer, som en finansiel enhed skal bestemme og vurdere, når den giver en kritisk eller vigtig funktion i underentreprise, således at bestemmelserne i stk. 2, litra a), får den rette virkning.

ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den [*EUT: Indsæt datoen 1 år efter ikrafttrædelsesdatoen*].

Kommissionen tillægges beføjelse til supplere denne forordning ved at vedtage de i første afsnit omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1095/2010 og (EU) nr. 1094/2010.

AFDELING II

TILSYNSRAMME FOR KRITISKE TREDJEPARTSUDBYDERE AF IKT-TJENESTER

Artikel 28

Udpegelse af kritiske tredjepartsudbydere af IKT-tjenester

1. ESA'erne skal via det fælles udvalg og efter henstilling fra det tilsynsforum, der er oprettet i henhold til artikel 29, stk. 1,

a) udpege de tredjepartsudbydere af IKT-tjenester, der er kritiske for finansielle enheder, under hensyntagen til kriterierne i stk. 2

b) udpege enten EBA, ESMA eller EIOPA som ledende tilsynsførende for hver af de kritiske tredjepartsudbydere af IKT-tjenester, afhængigt af, om den samlede værdi af aktiverne i de finansielle enheder, som gør brug af tjenester fra den pågældende tredjepartsudbyder af IKT-tjenester, og som er omfattet af henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 eller (EU) nr. 1095/2010, udgør mere end halvdelen af værdien af de samlede aktiver for alle de finansielle enheder, der benytter sig af tjenester fra den kritiske tredjepartsudbyder af IKT-tjenester, således som det fremgår af den konsoliderede balance, eller de individuelle balancer, hvor balancerne ikke er konsoliderede, for disse finansielle enheder.

2. Den udpegelse, der er omhandlet i stk. 1, litra a), skal baseres på samtlige følgende kriterier:

a) den systemiske indvirkning på stabiliteten, kontinuiteten eller kvaliteten af leveringen af finansielle tjenesteydelser, i tilfælde af at den pågældende tredjepartsudbyder af IKT-tjenester udsættes for et stort operationelt svigt, således at denne ikke kan levere sine tjenester, idet der tages hensyn til antallet af finansielle enheder, som den pågældende tredjepartsudbyder af IKT-tjenester leverer tjenesteydelser til

b) den systemiske karakter eller betydning af de finansielle enheder, der er afhængige af den pågældende tredjepartsudbyder af IKT-tjenester, som er vurderet i overensstemmelse med følgende parametre:

i) antallet af globale systemisk vigtige institutter (G-SII'er) eller andre systemisk vigtige institutter (O-SII'er), som er afhængige af den pågældende tredjepartsudbyder af IKT-tjenester

ii) den indbyrdes afhængighed mellem de i litra i) omhandlede G-SII'er eller O-SII'er og andre finansielle enheder, herunder situationer, hvor G-SII'erne eller O-SII'erne leverer finansielle infrastrukturtjenester til andre finansielle enheder

c) finansielle enheders afhængighed af de tjenester, der leveres af de pågældende tredjepartsudbydere af IKT-tjenester, i forbindelse med kritiske eller vigtige funktioner i finansielle enheder, som i sidste ende involverer den samme tredjepartsudbyder af IKT-tjenester, uanset om de benytter sig af disse tjenester direkte eller indirekte, ved hjælp af eller gennem underentrepriseordninger

d) i hvilket omfang tredjepartsudbyderen af IKT-tjenester kan erstattes under hensyntagen til følgende parametre:

i) manglen på reelle alternativer, selv delvist, på grund af det begrænsede antal tredjepartsudbydere af IKT-tjenester, der er aktive på et specifikt marked, eller den pågældende tredjepartsudbyder af IKT-tjenesters markedsandel, eller den involverede tekniske kompleksitet eller finesse, herunder i forbindelse med eventuelle egne teknologier, eller de særlige kendetegn ved tredjepartsudbyderen af IKT-tjenesters organisation eller aktivitet

ii) vanskeligheder med helt eller delvist at migrere de relevante data og arbejdsbyrden fra den pågældende tredjepartsudbyder af IKT-tjenester til andre tredjepartsudbydere af IKT-tjenester, enten på grund af betydelige finansielle omkostninger, tid eller andre ressourcer, som migreringen kan kræve, eller øgede IKT-risici eller andre operationelle risici, som den finansielle enhed kan blive eksponeret for ved en sådan migrering

e) antallet af medlemsstater, hvor den pågældende tredjepartsudbyder af IKT-tjenester leverer tjenester

f) antallet af medlemsstater, hvor finansielle enheder, som anvender den pågældende tredjepartsudbyder af IKT-tjenester, har aktiviteter.

3. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 50 for at supplere de i stk. 2 omhandlede kriterier.

4. Den udpegningsmekanisme, der er omhandlet i stk. 1, litra a), må først anvendes, når Kommissionen har vedtaget en delegeret retsakt i overensstemmelse med stk. 3.

5. Den udpegningsmekanisme, der er omhandlet i stk. 1, litra a), finder ikke anvendelse på tredjepartsudbydere af IKT-tjenester, som er underlagt tilsynsrammer, der er etableret med henblik på at understøtte de opgaver, der er omhandlet i artikel 127, stk. 2, i traktaten om Den Europæiske Unions funktionsmåde.

6. ESA'erne udarbejder, offentliggør og ajourfører årligt via det fælles udvalg listen over kritiske tredjepartsudbydere af IKT-tjenester på EU-plan.

7. Med henblik på stk. 1, litra a), videregiver de kompetente myndigheder på et årligt og aggregeret grundlag de rapporter, der er omhandlet i artikel 25, stk. 4, til det tilsynsforum, der er oprettet i henhold til artikel 29. Tilsynsforummet vurderer finansielle enheders afhængighed af tredjepartsudbydere af IKT-tjenester på grundlag af oplysninger, som det modtager fra de kompetente myndigheder.

8. Tredjepartsudbydere af IKT-tjenester, der ikke er opført på den i stk. 6 omhandlede liste, kan anmode om at blive optaget på denne liste.

   Med henblik på første afsnit indgiver tredjepartsudbyderen af IKT-tjenester en begrundet anmodning til EBA, ESMA eller EIOPA, som via det fælles udvalg beslutter, om det skal optage den pågældende tredjepartsudbyder af IKT-tjenester på denne liste i overensstemmelse med stk. 1, litra a).

   Den i andet afsnit omhandlede beslutning vedtages og meddeles tredjepartsudbyderen af IKT-tjenester senest 6 måneder efter modtagelsen af anmodningen.

9. Finansielle enheder må ikke gøre brug af en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland, som ville blive udpeget som kritisk i henhold til stk. 1, litra a), hvis denne havde hjemsted i Unionen.

Artikel 29

Tilsynsrammens struktur

1. Det fælles udvalg opretter i overensstemmelse med artikel 57 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 tilsynsforummet som et underudvalg med henblik på at støtte det arbejde, der udføres i det fælles udvalg og af den ledende tilsynsførende, der er omhandlet i artikel 28, stk. 1, litra b), med hensyn til IKT-tredjepartsrisici på tværs af finansielle sektorer. Tilsynsforummet udarbejder udkast til fælles holdninger og fælles retsakter vedtaget af det fælles udvalg inden for dette område.

   Tilsynsforummet drøfter regelmæssigt relevante udviklingstendenser vedrørende IKT-risici og -sårbarheder og fremmer en ensartet tilgang til overvågning af IKT-tredjepartsrisici på EU-plan.

2. Tilsynsforummet foretager på årsbasis en kollektiv vurdering af resultaterne og konklusionerne fra de tilsynsaktiviteter, der udføres for alle kritiske tredjepartsudbydere af IKT-tjenester, og fremmer koordineringsforanstaltninger for at øge finansielle enheders digitale operationelle modstandsdygtighed, fremme bedste praksis for håndtering af IKT-koncentrationsrisici og undersøge foranstaltninger til modvirkning af risikoafsmitning på tværs af sektorer.

3. I overensstemmelse med artikel 56, stk. 1, i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 forelægger tilsynsforummet omfattende benchmarks for kritiske tredjepartsudbydere af IKT-tjenester, som skal vedtages af det fælles udvalg som ESA'ernes fælles holdninger.

4. Tilsynsforummet er sammensat af formændene for ESA'erne og én repræsentant på højt niveau for personalet i den relevante kompetente myndighed fra hver medlemsstat. De administrerende direktører for hver ESA og en repræsentant fra henholdsvis Europa-Kommissionen, ESRB, ECB og ENISA deltager i tilsynsforummet som observatører.

5. I overensstemmelse med artikel 16 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 udsteder ESA'erne med henblik på denne afdeling retningslinjer for samarbejdet mellem ESA'erne og de kompetente myndigheder om de nærmere procedurer og betingelser, som vedrører varetagelsen af opgaver mellem de kompetente myndigheder og ESA'erne, samt nærmere oplysninger om den informationsudveksling, der er nødvendig for de kompetente myndigheder, således at de kan sikre opfølgning af de henstillinger, som ledende tilsynsførende i medfør af artikel 31, stk. 1, litra d), fremsætter over for kritiske tredjepartsudbydere af IKT-tjenester.

6. Kravene i denne afdeling berører ikke anvendelsen af direktiv (EU) 2016/1148 og andre af EU-regler om tilsyn, som finder anvendelse på udbydere af cloud computing-tjenester.

7. ESA'erne forelægger hvert år Europa-Parlamentet, Rådet og Kommissionen en rapport om anvendelsen af denne afdeling via det fælles udvalg og på grundlag af det forberedende arbejde, der udføres af tilsynsforummet.

Artikel 30

Den ledende tilsynsførendes opgaver

1. Den ledende tilsynsførende vurderer, om hver enkelt kritisk tredjepartsudbyder af IKT-tjenester har indført udførlige, forsvarlige og effektive regler, procedurer, mekanismer og ordninger til styring af de IKT-risici, som den kan udsætte finansielle enheder for.

2. Den i stk. 1 omhandlede vurdering omfatter følgende:

   a) IKT-krav, som navnlig skal garantere sikkerhed, tilgængelighed, kontinuitet, skalerbarhed og kvalitet for de tjenester, som den kritiske tredjepartsudbyder af IKT-tjenester leverer til finansielle enheder, samt at der til enhver til kan opretholdes høje standarder for sikkerhed, datafortrolighed og dataintegritet

b) fysisk sikkerhed, som bidrager til at garantere IKT-sikkerheden, herunder sikkerheden i lokaler, faciliteter og datacentre

c) risikostyringsprocesser, herunder politikker for IKT-risikostyring, planer for IKT-driftsstabilitet og IKT-katastrofeberedskabsplaner

d) ledelsesordninger, herunder en organisatorisk struktur med en klar, gennemsigtig og konsekvent ansvarsfordeling og regler om ansvarliggørelse, som muliggør en effektiv IKT-risikostyring

e) identifikation, overvågning og hurtig indberetning af IKT-relaterede hændelser til de finansielle enheder samt håndtering og afvikling af disse hændelser, navnlig cyberangreb

f) mekanismer for dataportabilitet, applikationsportabilitet og interoperabilitet, som sikrer en effektiv udøvelse af opsigelsesrettighederne for de finansielle enheder

g) afprøvning af IKT-systemer, -infrastruktur og -kontrolfunktioner

h) IKT-revisioner

i) anvendelse af relevante nationale og internationale standarder, som gælder for levering af IKT-tjenester til finansielle enheder.

3. På grundlag af den i stk. 1 omhandlede vurdering vedtager den ledende tilsynsførende en klar, detaljeret og begrundet individuel tilsynsplan for hver enkelt kritisk tredjepartsudbyder af IKT-tjenester. Denne plan skal hvert år meddeles den kritiske tredjepartsudbyder af IKT-tjenester.

4. Når de stk. 3 omhandlede årlige tilsynsplaner er blevet vedtaget og meddelt de kritiske tredjepartsudbydere af IKT-tjenester, kan de kompetente myndigheder kun træffe foranstaltninger, som vedrører kritiske tredjepartsudbydere af IKT-tjenester, efter aftale med den ledende tilsynsførende.

Artikel 31

Beføjelser, som tillægges den ledende tilsynsførende

1. Med henblik på varetagelsen af de i denne afdeling omhandlede opgaver tillægges den ledende tilsynsførende beføjelser til:

a) at anmode om alle relevante oplysninger og dokumentation i overensstemmelse med artikel 32

b) at foretage generelle undersøgelser og inspektioner i overensstemmelse med artikel 33 og 34

c) at anmode om rapporter efter afslutningen af tilsynsaktiviteterne med angivelse af de tiltag, der er iværksat, eller de afhjælpende foranstaltninger, som de kritiske tredjepartsudbydere af IKT-tjenester har truffet i forbindelse med de i litra d) omhandlede henstillinger

d) at fremsætte henstillinger vedrørende de områder, der er omhandlet i artikel 30, stk. 2, og navnlig følgende:

i) anvendelse af specifikke IKT-relaterede sikkerheds- og kvalitetskrav eller -processer, navnlig i forbindelse med udrulningen af programrettelser, opdateringer, kryptering og andre sikkerhedsforanstaltninger, som den ledende tilsynsførende betragter som relevante for at garantere IKT-sikkerheden for tjenester, der leveres til finansielle enheder

ii) anvendelse af betingelser og vilkår, herunder den tekniske gennemførelse heraf, i henhold til hvilke de kritiske tredjepartsudbydere af IKT-tjenester leverer tjenester til finansielle enheder, og som den ledende tilsynsførende betragter som relevante for at forhindre, at der genereres lokale fejl, eller at disse forstærkes, eller for at minimere eventuelle systemiske virkninger på tværs af EU's finansielle sektor i tilfælde af IKT-koncentrationsrisici

iii) efter den undersøgelse, der er foretaget i henhold til artikel 32 og 33 i underentrepriseordninger, herunder ordninger for videreoutsourcing, som de kritiske tredjepartsudbydere af IKT-tjenester planlægger at indgå med andre tredjepartsudbydere af IKT-tjenester eller med IKT-underleverandører med hjemsted i et tredjeland, eventuelle planlagte underentrepriser, herunder videreoutsourcing, hvor den ledende tilsynsførende finder, at yderligere underentrepriser kan udløse risici for den finansielle enheds levering af tjenesteydelser eller risici for den finansielle stabilitet

iv) at afholde sig fra at indgå endnu en underentrepriseordning, når følgende kumulative betingelser er opfyldt:

– den påtænkte underleverandør er en tredjepartsudbyder af IKT-tjenester eller en IKT-underleverandør med hjemsted i et tredjeland

– underentreprisen vedrører en kritisk eller vigtig funktion for den finansielle enhed.

2. Den ledende tilsynsførende hører tilsynsforummet forud for udøvelsen af de i stk. 1 omhandlede beføjelser.

3. Kritiske tredjepartsudbydere af IKT-tjenester samarbejder i god tro med den ledende tilsynsførende og bistår den ledende tilsynsførende med hensyn til varetagelsen af dennes opgaver.

4. Den ledende tilsynsførende kan pålægge tvangsbøder for at tvinge den kritiske tredjepartsudbyder af IKT-tjenester til at efterleve stk. 1, litra a)–c).

5. De i stk. 4 omhandlede tvangsbøder pålægges dagligt, indtil der er opnået efterlevelse, og i højst seks måneder efter meddelelsen heraf til den kritiske tredjepartsudbyder af IKT-tjenester.

6. De tvangsbøder, der beregnes fra den dato, der er anført i afgørelsen om pålæggelse af tvangsbøder, udgør 1 % af den gennemsnitlige daglige omsætning på verdensplan, som den kritiske tredjepartsudbydere af IKT-tjenester har realiseret i det foregående regnskabsår.

7. Tvangsbøder er af administrativ karakter og kan tvangsfuldbyrdes. Tvangsfuldbyrdelsen sker efter den borgerlige retsplejes regler i den medlemsstat, på hvis område inspektioner og adgang skal finde sted. Domstole i den pågældende medlemsstat har kompetence til at træffe afgørelse om klager vedrørende uregelmæssigheder i forbindelse med tvangsfuldbyrdelsen. Beløbene for tvangsbøderne overføres til Den Europæiske Unions almindelige budget.

8. ESA'erne offentliggør alle de pålagte tvangsbøder, medmindre en sådan offentliggørelse vil være til alvorlig skade for de finansielle markeder eller forvolde de involverede parter uforholdsmæssig stor skade.

9. Inden der pålægges tvangsbøder i henhold til stk. 4, giver den ledende tilsynsførende repræsentanter for den kritiske tredjepartsudbyder af IKT-tjenester, som er genstand for proceduren, mulighed for at blive hørt om resultaterne og baserer sine afgørelser udelukkende på resultater, som den kritiske tredjepartsudbyder af IKT-tjenester, der er genstand for proceduren, har haft lejlighed til at fremsætte bemærkninger til. Retten til forsvar for de personer, som er genstand for proceduren, skal respekteres fuldt ud under procedureforløbet. De har ret til aktindsigt i sagsakterne med forbehold af andre personers berettigede interesse i, at deres forretningshemmeligheder ikke afsløres. Retten til aktindsigt omfatter ikke fortrolige oplysninger eller den ledende tilsynsførendes interne forberedende dokumenter.

Artikel 32
Anmodning om oplysninger

1. Den ledende tilsynsførende kan efter simpel anmodning eller ved en afgørelse kræve, at de kritiske tredjepartsudbydere af IKT-tjenester fremlægger alle de oplysninger, der er nødvendige for, at den ledende tilsynsførende kan varetage sine opgaver i henhold til denne forordning, herunder alle relevante forretningsdokumenter eller operationelle dokumenter, kontrakter, politikdokumentation, rapporter om IKT-sikkerhedsrevision, indberetninger af IKT-relaterede hændelser samt oplysninger om parter, som den kritiske tredjepartsudbyder af IKT-tjeneste har outsourcet operationelle funktioner eller aktiviteter til.

2. Når den ledende tilsynsførende sender en simpel anmodning om oplysninger i henhold til stk. 1, skal denne

   a) henvise til denne artikel som retsgrundlag for anmodningen

   b) angive formålet med anmodningen

   c) præcisere, hvilke oplysninger der kræves

   d) fastsætte en frist for tilvejebringelsen af oplysningerne

e) meddele repræsentanten for den kritiske tredjepartsudbyder af IKT-tjenester, som anmodes om oplysningerne, at vedkommende ikke er forpligtet til at tilvejebringe oplysningerne, men at oplysningerne, såfremt vedkommende frivilligt fremlægger dem, ikke må være ukorrekte eller vildledende.

3. Ved krav om tilvejebringelse af oplysninger i henhold til stk. 1, skal den ledende tilsynsførende

a) henvise til denne artikel som retsgrundlag for anmodningen

b) angive formålet med anmodningen

c) præcisere, hvilke oplysninger der kræves

d) fastsætte en frist for tilvejebringelsen af oplysningerne

e) angive de tvangsbøder, der er fastsat i artikel 31, stk. 4, og som finder anvendelse, hvis de ønskede oplysninger er ufuldstændige

f) oplyse om retten til at appellere afgørelsen for ESA'ernes klagenævn og om retten til at indbringe en klage over afgørelsen for Den Europæiske Unions Domstol ("Domstolen") i overensstemmelse med artikel 60 og 61 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

4. De ønskede oplysninger udleveres af repræsentanter for kritiske tredjepartsudbydere af IKT-tjenester. Behørigt befuldmægtigede advokater kan udlevere de ønskede oplysninger på deres klienters vegne. Den kritiske tredjepartsudbyder af IKT-tjenester bærer det fulde ansvar for, at oplysningerne er fuldstændige, korrekte og ikke vildledende.

5. Den ledende tilsynsførende sender straks en kopi af afgørelsen om at udlevere oplysninger til de kompetente myndigheder for de finansielle enheder, der benytter sig af tjenester, som de kritiske tredjepartsudbydere af IKT-tjenester leverer.

Artikel 33
Generelle undersøgelser

1. For at varetage sine opgaver i henhold til denne forordning kan den ledende tilsynsførende, som bistås af det undersøgelseshold, der er omhandlet i artikel 34, stk. 1, foretage de nødvendige undersøgelser af tredjepartsudbydere af IKT-tjenester.

2. Den ledende tilsynsførende tillægges beføjelse til

a) at undersøge optegnelser, data, procedurer og eventuelt andet materiale, som har betydning for varetagelsen af dennes opgaver, uanset det medium, hvorpå de er lagret

b) at tage eller erhverve bekræftede genparter eller udskrifter af sådanne optegnelser, data, procedurer og andet materiale

c) at indkalde repræsentanter for den kritiske tredjepartsudbyder af IKT-tjenester med henblik på mundtlige eller skriftlige forklaringer på forhold eller

dokumenter, der vedrører undersøgelsens genstand og formål, og at optage svarene

d) at udspørge enhver anden fysisk eller juridisk person, der indvilliger heri, med det formål at indsamle oplysninger om undersøgelsens genstand

e) at anmode om oplysninger om telefonsamtaler og datatrafik.

3. De embedsmænd og andre personer, som den ledende tilsynsførende har bemyndiget til at foretage de i stk. 1 omhandlede undersøgelser, udøver deres beføjelser efter fremlæggelse af en skriftlig tilladelse, som angiver genstanden for undersøgelsen og formålet hermed.

Denne tilladelse skal også indeholde oplysninger om de tvangsbøder, der er omhandlet i artikel 31, stk. 4, hvis de krævede optegnelser, data, procedurer eller andet materiale eller svarene på de spørgsmål, der stilles til repræsentanter for tredjepartsudbyderne af IKT-tjenester, ikke fremlægges eller er ufuldstændige.

4. Repræsentanterne for tredjepartsudbyderne af IKT-tjenester skal lade sig underkaste undersøgelserne på grundlag af en afgørelse truffet af den ledende tilsynsførende. Afgørelsen skal angive undersøgelsens genstand og formål, de tvangsbøder, der er omhandlet i artikel 31, stk. 4, de retsmidler, der er tilgængelige i henhold til henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010, og retten til at indbringe en klage over afgørelsen for Domstolen.

5. De ledende tilsynsførende underretter i god tid før undersøgelsen de kompetente myndigheder for de finansielle enheder, som anvender den pågældende tredjepartsudbyder af IKT-tjenester, om undersøgelsen og om de bemyndigede personers identitet.

Artikel 34
Inspektioner på stedet

1. Med henblik på at varetage sine opgaver i henhold til denne forordning kan den ledende tilsynsførende, som bistås af de undersøgelseshold, der er omhandlet i artikel 35, stk. 1, foretage alle nødvendige inspektioner på stedet i alle forretningslokaler, arealer eller ejendomme, som tilhører tredjepartsudbyderne af IKT-tjenester, f.eks. hovedkontorer, operationscentraler, sekundære lokaler, samt foretage eksterne inspektioner.

2. De embedsmænd og andre personer, som den ledende tilsynsførende har bemyndiget til at foretage inspektion på stedet, kan betræde alle sådanne forretningslokaler, arealer eller ejendomme og skal tillægges alle beføjelser til at forsegle alle forretningslokaler og bøger eller registre i det for inspektionen nødvendige tidsrum og omfang.

De udøver deres beføjelser efter fremlæggelse af en skriftlig tilladelse, der angiver genstanden for og formålet med inspektionen og de tvangsbøder, der er omhandlet i artikel 31, stk. 4, hvis repræsentanterne for de berørte IKT-tjenesteleverandører ikke lader sig underkaste inspektionen.

3. De ledende tilsynsførende underretter i god tid før inspektionen de kompetente myndigheder for de finansielle enheder, som anvender den pågældende tredjepartsudbyder af IKT-tjenester.

4. Inspektioner skal omfatte hele viften af relevante IKT-systemer, netværk, udstyr, oplysninger og data, der enten anvendes til eller bidrager til leveringen af tjenester til finansielle enheder.

5. De ledende tilsynsførende underretter kritiske tredjepartsudbydere af IKT-tjenester i rimelig tid før enhver planlagt inspektion, medmindre en sådan underretning ikke er mulig på grund af en nød- eller krisesituation, eller hvis det vil føre til en situation, hvor inspektionen eller revisionen ikke længere vil være effektiv(t).

6. Den kritiske tredjepartsudbyder af IKT-tjenester skal lade sig underkaste inspektioner på stedet, som er påbudt i henhold til en afgørelse truffet af den ledende tilsynsførende. Afgørelsen angiver inspektionens genstand og formål, fastsætter tidspunktet for dets påbegyndelse og oplyser om de tvangsbøder, der er foreskrevet i artikel 31, stk. 4, de retsmidler, der er tilgængelige i henhold til henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010, og om retten til at indbringe en klage over afgørelsen for Domstolen.

7. Hvis de embedsmænd og andre personer, der er bemyndiget af den ledende tilsynsførende, konstaterer, at en kritisk tredjepartsudbyder af IKT-tjenester gør indsigelse mod en inspektion, der er påbudt i henhold til denne artikel, underretter den ledende tilsynsførende den kritiske tredjepartsudbyder af IKT-tjenester om konsekvenserne af en sådan indsigelse, herunder muligheden for, at de kompetente myndigheder for de relevante finansielle enheder kan opsige de kontraktlige ordninger, der er indgået med denne kritiske tredjepartsudbyder af IKT-tjenester.

Artikel 35
Løbende tilsyn

1. Når de ledende tilsynsførende foretager generelle undersøgelser eller inspektioner på stedet, skal de bistås af et fælles undersøgelseshold, som er oprettet for hver af de kritiske tredjepartsudbydere af IKT-tjeneste.

2. Det fælles undersøgelseshold, der er omhandlet i stk. 1, skal bestå af medarbejdere fra den ledende tilsynsførende og fra de relevante kompetente myndigheder, der fører tilsyn med de finansielle enheder, som den kritiske tredjepartsudbyder af IKT-tjenester leverer tjenester til; de inddrages i forberedelsen og gennemførelsen af tilsynsaktiviteterne med højst 10 medlemmer. Alle medlemmer af det fælles undersøgelseshold skal have ekspertise med hensyn til IKT-risici og operationelle risici. Arbejdet i det fælles undersøgelseshold koordineres af en udpeget medarbejder fra ESA ("koordinatoren for den ledende tilsynsførende").

3. ESA'erne udarbejder via det fælles udvalg fælles udkast til reguleringsmæssige tekniske standarder for yderligere at præcisere udpegelsen af de medlemmer af det fælles undersøgelseshold, som kommer fra de relevante kompetente myndigheder, samt undersøgelsesholdets opgaver og arbejdsordninger. ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den [*EUT: Indsæt datoen 1 år efter ikrafttrædelsesdatoen*].

Kommissionen tillægges beføjelse til at vedtage de i første afsnit omhandlede reguleringsmæssige tekniske standarder i overensstemmelse med artikel 10-14 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

4. Inden for 3 måneder efter fuldførelsen af en undersøgelse eller en inspektion på stedet og efter høring af tilsynsforummet vedtager den ledende tilsynsførende henstillinger, som den ledende tilsynsførende skal meddele den berørte kritiske tredjepartsudbyder af IKT-tjenester, i henhold til de i artikel 31 omhandlede beføjelser.

5. De i stk. 4 omhandlede henstillinger meddeles omgående den berørte kritiske tredjepartsudbyder af IKT-tjenester og de kompetente myndigheder for de finansielle enheder, som den leverer tjenester til.

Med henblik på at varetage tilsynsaktiviteter kan ledende tilsynsførende tage hensyn til eventuelle relevante tredjepartscertificeringer og IKT-tredjeparters interne eller eksterne revisionspåtegninger, som den berørte kritiske tredjepartsudbyder af IKT-tjenester har stillet til rådighed.

Artikel 36

Harmonisering af de betingelser, der muliggør gennemførelsen af tilsyn

1. ESA'erne udarbejder via det fælles udvalg udkast til reguleringsmæssige tekniske standarder for at præcisere følgende:

a) de oplysninger, som en kritisk tredjepartsudbyder af IKT-tjenester skal fremlægge i sin ansøgning om frivillig deltagelse, jf. artikel 28, stk. 8

b) indholdet og formatet af de rapporter, der kan anmodes om med henblik på artikel 31, stk. 1, litra c)

c) fremlæggelsen af de oplysninger, herunder struktur, formater og metoder, som en kritisk tredjepartsudbyder af IKT-tjenester skal indgive, offentliggøre eller aflægge rapport om i henhold til artikel 31, stk. 1

d) de nærmere oplysninger om de kompetente myndigheders vurdering af foranstaltningers, som kritiske tredjepartsudbydere af IKT-tjenester har truffet, på grundlag af henstillinger fra ledende tilsynsførende, jf. artikel 37, stk. 2.

2. ESA'erne forelægger disse udkast til reguleringsmæssige tekniske standarder for Kommissionen senest den 1. januar 20xx [*EUT: Indsæt datoen 1 år efter ikrafttrædelsesdatoen*].

Kommissionen tillægges beføjelse til supplere denne forordning ved at vedtage de i første afsnit omhandlede reguleringsmæssige tekniske standarder i overensstemmelse

med den procedure, der er fastsat i artikel 10-14 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikel 37

De kompetente myndigheders opfølgning

1. Inden for en frist på 30 kalenderdage efter modtagelsen af de henstillinger, der er fremsat af tilsynsførende i henhold til artikel 31, stk. 1, litra d), underretter de kritiske tredjepartsudbydere af IKT-tjenester den ledende tilsynsførende om, hvorvidt de agter at følge disse henstillinger. De ledende tilsynsførende videregiver straks disse oplysninger til de kompetente myndigheder.

2. De kompetente myndigheder overvåger, om de finansielle enheder tager hensyn til de risici, der er identificeret i de henstillinger, der er meddelt kritiske tredjepartsudbydere af IKT-tjenester i henhold til artikel 31, stk. 1, litra d).

3. De kompetente myndigheder kan i henhold til artikel 44 kræve, at finansielle enheder midlertidigt suspenderer, enten helt eller delvist, anvendelsen eller udrulningen af en tjeneste, som den kritiske tredjepartsudbyder af IKT-tjenester leverer, indtil de risici, der er identificeret i de henstillinger, der er meddelt de kritiske IKT-tredjepartsleverandører, er blevet afhjulpet. De kan om nødvendigt kræve, at finansielle enheder helt eller delvist opsiger de relevante kontraktlige ordninger, der er indgået med de kritiske tredjepartsudbydere af IKT-tjenester.

4. Når de kompetente myndigheder træffer de i stk. 3 omhandlede afgørelser, tager de hensyn til typen og omfanget af den risiko, som ikke afhjælpes af den kritiske tredjepartsudbyder af IKT-tjenester, samt alvoren af den manglende overholdelse, under hensyntagen til følgende kriterier:

   a) den manglende overholdelses grovhed og varighed

   b) hvorvidt den manglende overholdelse har afsløret alvorlige svagheder i de procedurer, de forvaltningssystemer, den risikostyring og de interne kontroller, som den kritiske tredjepartsudbyder af IKT-tjenester varetager

   c) om økonomisk kriminalitet blev fremmet eller foranlediget af eller på anden måde kan tilskrives den manglende overholdelse

   d) hvorvidt den manglende overholdelse er forsætlig eller skyldes uagtsomhed.

5. De kompetente myndigheder orienterer regelmæssigt de ledende tilsynsførende om de tilgange og foranstaltninger, de har iværksat i forbindelse med deres tilsynsopgaver vedrørende finansielle enheder, samt om de kontraktlige foranstaltninger, som sidstnævnte har truffet, når den kritiske tredjepartsudbyder af IKT-tjenester kun delvist eller slet ikke har tilsluttet sig de henstillinger, som den ledende tilsynsførende har meddelt dem.

Artikel 38

Tilsynsgebyrer

1. ESA'erne opkræver gebyrer hos kritiske tredjepartsudbydere af IKT-tjenester, som fuldt ud dækker de nødvendige udgifter i forbindelse med varetagelsen af tilsynsopgaver i henhold til denne forordning, herunder godtgørelse af eventuelle omkostninger, der kan opstå som følge af det arbejde, der udføres af kompetente myndigheder, som deltager i tilsynsudvalget i henhold til artikel 35.

   Det gebyrbeløb, der opkræves hos en kritisk tredjepartsudbyder af IKT-tjenester, skal dække alle administrative omkostninger og stå i et rimeligt forhold til dennes omsætning.

2. Kommissionen tillægges beføjelser til at vedtage en delegeret retsakt i overensstemmelse med artikel 50 med henblik på at supplere denne forordning ved at fastsætte gebyrbeløbene og betalingsmåden.

Artikel 39

Internationalt samarbejde

1. EBA, ESMA og EIOPA kan i overensstemmelse med artikel 33 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 indgå administrative ordninger med tredjelandes regulerings- og tilsynsmyndigheder for at fremme det internationale samarbejde om IKT-risici på tværs af forskellige finansielle sektorer, navnlig ved at udvikle bedste praksis for gennemgang af fremgangsmåder og kontroller forbundet med IKT-risikostyring, afhjælpende foranstaltninger og indsatsen i forbindelse med hændelser.

2. ESA'erne forelægger hvert femte år via det fælles udvalg en fortrolig rapport for Europa-Parlamentet, Rådet og Kommissionen med en sammenfatning af resultaterne af de relevante drøftelser, der er ført med de i stk. 1 omhandlede tredjelandes myndigheder, med fokus på udviklingen inden for IKT-tredjepartsrisici og konsekvenserne for den finansielle stabilitet, markedets integritet, investorbeskyttelsen eller det indre markeds funktionsmåde.

KAPITEL VI

ORDNINGER FOR INFORMATIONSUDVEKSLING

Artikel 40

Ordninger for informationsudveksling af oplysninger og efterretninger om cybertrusler

1. De finansielle enheder kan indbyrdes udveksle oplysninger og efterretninger om cybertrusler, herunder kompromitteringsindikatorer, taktikker, teknikker og procedurer, cybersikkerhedsvarsler og konfigurationsværktøjer, i det omfang en sådan udveksling af oplysninger og efterretninger:

a) har til formål at forbedre finansielle enheders digitale operationelle modstandsdygtighed, navnlig ved at øge bevidstheden om cybertrusler, begrænse eller hindre cybertruslernes spredningsevne, understøtte finansielle enheders udbud af forsvarskapaciteter, teknikker til detektion af trusler, strategier for afbødning eller indsats- og genopretningsfaser

b) finder sted inden for pålidelige grupper af finansielle enheder

c) gennemføres gennem ordninger for informationsudveksling, der beskytter de udvekslede oplysningers potentielt sensitive karakter, og som er omfattet af regler om god forretningsskik med fuld respekt for forretningshemmeligheder, beskyttelse af personoplysninger[48] og retningslinjer for konkurrencepolitikken[49].

2. Med henblik på stk. 1, litra c), fastlægger ordningerne for informationsudveksling betingelserne for deltagelse og fastsætter, hvor det er relevant, de nærmere bestemmelser om inddragelse af offentlige myndigheder og om den egenskab, i hvilken sidstnævnte kan indgå i ordninger for informationsudveksling samt om operationelle elementer, herunder anvendelsen af særlige IT-platforme.

3. De finansielle enheder underretter de kompetente myndigheder om deres deltagelse i de i stk. 1 omhandlede ordninger for informationsudveksling efter validering af deres medlemskab eller i givet fald ophør af deres medlemskab, når sidstnævnte træder i kraft.

KAPITEL VII

KOMPETENTE MYNDIGHEDER

Artikel 41

Kompetente myndigheder

Uden at dette berører bestemmelserne i denne forordnings kapitel V, afdeling II, om tilsynsrammen for kritiske tredjepartsudbydere af IKT-tjenester, sikrer følgende kompetente myndigheder overholdelse af de forpligtelser, der er fastsat i denne forordning, i overensstemmelse med de beføjelser, som tillægges dem ved de respektive retsakter:

a) for kreditinstitutter: den kompetente myndighed, der er udpeget i henhold til artikel 4 i direktiv 2013/36/EU, uden at dette berører de særlige opgaver, som overdrages til ECB ved forordning (EU) nr. 1024/2013

---

48 I overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

49 Kommissionens meddelelse — Retningslinjer for anvendelsen af artikel 101 i traktaten om Den Europæiske Unions funktionsmåde på horisontale samarbejdsaftaler (EUT C 11 af 14.1.2011, s. 1).

b) for betalingstjenesteudbydere: den kompetente myndighed, der er udpeget i henhold til artikel 22 i direktiv (EU) 2015/2366

c) for e-pengeinstitutter: den kompetente myndighed, der er udpeget i henhold til artikel 37 i direktiv 2009/110/EF

d) for investeringsselskaber: den kompetente myndighed, der er udpeget i henhold til artikel 4 i direktiv (EU) 2019/2034

e) for udbydere af kryptoaktivtjenester, udstedere af kryptoaktiver, udstedere af aktivbaserede tokens og udstedere af signifikante aktivbaserede tokens: den kompetente myndighed, der er udpeget i overensstemmelse med artikel 3, stk. 1, litra ee), første led, i [Mica-forordning (EU) 20xx/xx]

f) for værdipapircentraler: den kompetente myndighed, der er udpeget i henhold til artikel 11 i forordning (EU) nr. 909/2014

g) for værdipapircentraler: den kompetente myndighed, der er udpeget i henhold til artikel 22 i forordning (EU) nr. 648/2012

h) for markedspladser og udbydere af dataindberetningstjenester: den kompetente myndighed, der er udpeget i henhold til artikel 67 i direktiv 2014/65/EU

i) for transaktionsregistre: den kompetente myndighed, der er udpeget i henhold til artikel 55 i forordning (EU) nr. 648/2012

j) for forvaltere af alternative investeringsfonde: den kompetente myndighed, der er udpeget i henhold til artikel 44 i direktiv 2011/61/EU

k) for administrationsselskaber: den kompetente myndighed, der er udpeget i henhold til artikel 97 i direktiv 2009/65/EF

l) for forsikrings- og genforsikringsselskaber: den kompetente myndighed, der er udpeget i henhold til artikel 30 i direktiv 2009/138/EF

m) for forsikringsformidlere, genforsikringsformidlere og accessoriske forsikringsformidlere: den kompetente myndighed, der er udpeget i henhold til artikel 12 i direktiv (EU) 2016/97

n) for arbejdsmarkedsrelaterede pensionskasser: den kompetente myndighed, der er udpeget i henhold til artikel 47 i direktiv (EU) 2016/2341

o) for kreditvurderingsbureauer: den kompetente myndighed, der er udpeget i henhold til artikel 21 i forordning (EF) nr. 1060/2009

p) for revisorer og revisionsfirmaer: den kompetente myndighed, der er udpeget i henhold til artikel 3, stk. 2, og artikel 32 i direktiv 2006/43/EF

q) for administratorer af kritiske benchmarks: den kompetente myndighed, der er udpeget i henhold til artikel 40 og 41 i *forordning (EU) 20xx/xx*

r) for udbydere af crowdfundingtjenester: den kompetente myndighed, der er udpeget i henhold til bilag x i *forordning (EU) 20xx/xx*

s) for securitiseringsregistre: den kompetente myndighed, der er udpeget i henhold til artikel 10 og artikel 14, stk. 1, i forordning (EU) 2017/2402.

Artikel 42

Samarbejde med strukturer og myndigheder, der er oprettet ved direktiv (EU) 2016/1148

1. For at fremme samarbejde og muliggøre tilsynsmæssig udveksling mellem de kompetente myndigheder, der er udpeget i henhold til denne forordning, og den samarbejdsgruppe, der er nedsat ved artikel 11 i direktiv (EU) 2016/1148, kan ESA'erne og de kompetente myndigheder anmode om at blive inddraget i samarbejdsgruppens arbejde.

2. De kompetente myndigheder kan, hvor det er relevant, rådføre sig med det centrale kontaktpunkt og de nationale enheder, der håndterer IT-sikkerhedshændelser, jf. henholdsvis artikel 8 og 9 i direktiv (EU) 2016/1148.

Artikel 43

Grænseoverskridende simuleringsøvelser, kommunikation og samarbejde inden for finans

1. ESA'erne kan via det fælles Udvalg og i samarbejde med de kompetente myndigheder, ECB og ESRB indføre mekanismer, der gør det muligt at udveksle effektive fremgangsmåder på tværs af finansielle sektorer for at forbedre situationskendskabet og identificere fælles cybersårbarheder og risici på tværs af sektorer.

   De kan udvikle simuleringsøvelser for krisestyring og beredskab, der omfatter cyberangrebsscenarier, med henblik på at udvikle kommunikationskanaler og gradvist muliggøre en effektiv koordineret indsats på EU-plan i tilfælde af en større grænseoverskridende IKT-relateret hændelse eller dermed forbundet trussel, som har systemiske virkninger for Unionens finansielle sektor som helhed.

   Disse simuleringsøvelser kan, alt efter hvad der er relevant, også tjene til at teste den finansielle sektors afhængighed af andre økonomiske sektorer.

2. De kompetente myndigheder, EBA, ESMA eller EIOPA og ECB samarbejder tæt med hinanden og udveksler oplysninger med henblik på at varetage deres opgaver i henhold til artikel 42-48. De koordinerer deres tilsyn tæt for at identificere og afhjælpe overtrædelser denne forordning, udvikle og fremme bedste praksis, lette samarbejdet, fremme en konsekvent fortolkning og tilvejebringe vurderinger på tværs af jurisdiktioner i tilfælde af eventuelle tvister.

Artikel 44

Administrative sanktioner og afhjælpende foranstaltninger

1. De kompetente myndigheder tillægges alle de nødvendige tilsynsmæssige beføjelser, undersøgelses- og sanktionsbeføjelser, således at de kan opfylde deres forpligtelser i henhold til denne forordning.

2. De i stk. 1 omhandlede beføjelser skal mindst omfatte beføjelser til:

a) at få adgang til ethvert dokument eller data i enhver form, som den kompetente myndighed anser for relevant for varetagelsen af sine opgaver, og modtage eller tage en kopi deraf

b) at gennemføre inspektioner eller undersøgelser på stedet

c) at kræve korrigerende foranstaltninger og afhjælpende foranstaltninger for overtrædelser af kravene i denne forordning.

3. Uden at dette berører medlemsstaternes ret til at pålægge strafferetlige sanktioner i henhold til artikel 46, fastsætter medlemsstaterne bestemmelser om passende administrative sanktioner og afhjælpende foranstaltninger for overtrædelser af denne forordning og sikrer en effektiv gennemførelse heraf.

Disse sanktioner eller foranstaltninger skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

4. Medlemsstaterne tillægger de kompetente myndigheder beføjelse til at anvende mindst følgende administrative sanktioner eller afhjælpende foranstaltninger for overtrædelser af denne forordning:

a) at udstede et påbud om, at den fysiske eller juridiske person bringer den udviste adfærd til ophør og afholder sig fra at gentage en sådan adfærd

b) at kræve midlertidigt eller permanent ophør med en praksis eller adfærd, som den kompetente myndighed anser for at stride mod bestemmelserne i denne forordning, og forhindre, at en sådan praksis eller adfærd gentager sig

c) at træffe enhver form for foranstaltning, herunder af pekuniær karakter, for at sikre, at de finansielle enheder fortsat overholder de retlige krav

d) i det omfang den nationale lovgivning tillader det, at kræve udlevering af eksisterende optegnelser over datatrafik, som en telekommunikationsoperatør er i besiddelse af, når der foreligger en rimelig mistanke om en overtrædelse af denne forordning, og hvor sådanne optegnelser kan være relevante for en undersøgelse af overtrædelser af denne forordning og

e) at udsende offentliggøre meddelelser, herunder offentlige erklæringer, der angiver den fysiske eller juridiske persons identitet og overtrædelsens art.

5. Såfremt de bestemmelser, der er omhandlet i stk. 2, litra c), og i stk. 4, finder anvendelse på juridiske personer, giver medlemsstaterne de kompetente myndigheder beføjelse til i overensstemmelse med betingelserne i national ret at anvende de administrative sanktioner og afhjælpende foranstaltninger på medlemmer af ledelsesorganet samt andre personer, som i henhold til national ret er ansvarlige for overtrædelsen.

6. Medlemsstaterne sikrer, at enhver afgørelse om pålæggelse af administrative sanktioner eller afhjælpende foranstaltninger, jf. stk. 2, litra c), er behørigt begrundet og kan påklages.

Artikel 45

Udøvelse af beføjelsen til at pålægge administrative sanktioner og afhjælpende foranstaltninger

1. De kompetente myndigheder udøver beføjelsen til at pålægge de administrative sanktioner og afhjælpende foranstaltninger, der er omhandlet i artikel 44, i overensstemmelse med nationale lovrammer, alt efter hvad der er relevant:

   a) direkte

   b) i samarbejde med andre myndigheder

   c) under eget ansvar ved delegation til andre myndigheder

   d) ved anmodning til de kompetente judicielle myndigheder.

2. De kompetente myndigheder tager ved valget af arten af og niveauet for en administrativ sanktion eller afhjælpende foranstaltning, der pålægges i henhold til artikel 44, hensyn til, i hvilken grad overtrædelsen er forsætlig eller skyldes uagtsomhed, og alle relevante omstændigheder, herunder, hvis det er relevant:

   a) overtrædelsens væsentlighed, grovhed og varighed

   b) graden af ansvar hos den fysiske eller juridiske person, der er ansvarlig for overtrædelsen

   c) den ansvarlige fysiske eller juridiske persons finansielle styrke

   d) omfanget af den ansvarlige fysiske eller juridiske persons fortjeneste eller undgåede tab, såfremt disse beløb kan beregnes

   e) de tab for tredjeparter, som skyldes overtrædelsen, såfremt disse beløb kan beregnes

   f) viljen hos den fysiske eller juridiske person til at samarbejde med den kompetente myndighed, uden at det dog tilsidesætter kravet om tilbagebetaling af den pågældende persons fortjeneste eller undgåede tab

   g) overtrædelser, som den ansvarlige fysiske eller juridiske person tidligere har begået.

Artikel 46

Strafferetlige sanktioner

1. Medlemsstaterne kan beslutte ikke at fastsætte bestemmelser om administrative sanktioner eller afhjælpende foranstaltninger for overtrædelser, der er omfattet af strafferetlige sanktioner i henhold til national ret.

2. Hvis medlemsstaterne har valgt at fastsætte strafferetlige sanktioner for overtrædelser af denne forordning, sikrer de, at der er truffet passende foranstaltninger, således at

de kompetente myndigheder har alle de nødvendige beføjelser til at holde kontakt til de retlige, retsforfølgende eller strafferetlige myndigheder inden for deres jurisdiktion for at indhente specifikke oplysninger om strafferetlige efterforskninger eller straffesager, der er indledt for overtrædelser af denne forordning, og til at give andre kompetente myndigheder samt EBA, ESMA eller EIOPA de samme oplysninger, således at disse kan opfylde deres forpligtelser til at samarbejde med henblik på anvendelsen af denne forordning.

Artikel 47

Meddelelsespligt

Medlemsstaterne giver senest [*EUT: Indsæt datoen 1 år efter ikrafttrædelsesdatoen*] Kommissionen, ESMA, EBA, og EIOPA meddelelse om de love og administrative bestemmelser, herunder relevante strafferetlige bestemmelser, som gennemfører dette kapitel. Medlemsstaterne meddeler uden unødigt ophold Kommissionen, ESMA, EBA, og EIOPA om eventuelle senere ændringer heraf.

Artikel 48

Offentliggørelse af administrative sanktioner

1. De kompetente myndigheder offentliggør uden unødigt ophold på deres officielle websteder enhver afgørelse om pålæggelse af en administrativ sanktion, som ikke kan påklages, efter at modtageren af sanktionen er blevet underrettet om afgørelsen.

2. Den i stk. 1 omhandlede offentliggørelse omfatter oplysninger om overtrædelsens type og art, de ansvarlige personers identitet samt de pålagte sanktioner.

3. Hvis den kompetente myndighed efter en vurdering i det enkelte tilfælde finder, at offentliggørelse af identiteten, hvis der er tale om juridiske personer, eller af identiteten og personoplysninger, hvis der er tale om fysiske personer, ikke vil stå i rimeligt forhold til sanktionen, vil bringe de finansielle markeders stabilitet eller gennemførelsen af en igangværende strafferetlig efterforskning i fare eller, i det omfang skaden kan fastslås, vil forvolde uforholdsmæssigt stor skade på den involverede person, vedtager den en af følgende løsninger med hensyn til afgørelsen om at pålægge en administrativ sanktion:

   a) udsætte offentliggørelsen heraf indtil det tidspunkt, hvor der ikke længere findes nogen begrundelse for at undlade offentliggørelse

   b) offentliggøre den anonymt i overensstemmelse med national lovgivning eller

   c) undlade at offentliggøre den, hvis mulighederne i litra a) og b) enten anses for at være utilstrækkelige til at sikre, at de finansielle markeders stabilitet ikke bringes i fare, eller hvis en sådan offentliggørelse ikke står i et rimeligt forhold til lempelsen af den pålagte sanktion.

4. I tilfælde af en afgørelse om at offentliggøre en administrativ sanktion anonymt i overensstemmelse med stk. 3, litra b), kan offentliggørelsen af de relevante oplysninger udskydes.

5. Hvis en kompetent myndighed offentliggør en afgørelse om at pålægge en administrativ sanktion, der kan indbringes for de relevante judicielle myndigheder, lægger de kompetente myndigheder straks denne oplysning på deres officielle websted sammen med eventuelle efterfølgende oplysninger om resultatet af denne indbringelse på et senere tidspunkt. En judiciel afgørelse, som annullerer en afgørelse om at pålægge en administrativ sanktion, skal også offentliggøres.

6. Kompetente myndigheder sikrer, at enhver offentliggørelse som omhandlet i stk. 1-4 er tilgængelig på deres officielle websted i mindst fem år efter offentliggørelsen. Personoplysninger indeholdt i offentliggørelsen forbliver kun på den kompetente myndigheds officielle websted i det tidsrum, hvor det er nødvendigt, i overensstemmelse med de gældende databeskyttelsesregler.

Artikel 49

Tavshedspligt

1. Enhver fortrolig oplysning, der modtages, udveksles eller videregives i henhold til denne forordning, er underlagt de i stk. 2 omhandlede betingelser vedrørende tavshedspligt.

2. Tavshedspligten gælder for alle personer, der arbejder eller har arbejdet for de kompetente myndigheder i henhold til denne forordning eller for en myndighed, en markedsdeltager eller en fysisk eller juridisk person, som disse kompetente myndigheder har overdraget sine beføjelser til, herunder revisorer og sagkyndige, der har indgået en kontrakt med disse.

3. Oplysninger, der er omfattet af tavshedspligt, må ikke videregives til nogen anden person eller myndighed, medmindre der er hjemmel dertil i medfør af EU-ret eller national ret.

4. Alle oplysninger, der udveksles mellem de kompetente myndigheder i henhold til denne forordning, og som vedrører forretnings- eller driftsmæssige betingelser og andre økonomiske eller personlige anliggender, betragtes som fortrolige og er underlagt krav om tavshedspligt, undtagen når den kompetente myndighed på det tidspunkt, hvor oplysningerne blev meddelt, har erklæret, at disse oplysninger kan videregives, eller når videregivelse er nødvendig i forbindelse med en eventuel retsforfølgning.

KAPITEL VIII

DELEGEREDE RETSAKTER

Artikel 50

Udøvelse af de delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 28, stk. 3, og artikel 38, stk. 2, tillægges Kommissionen for en periode på fem år fra den [*EUT: Indsæt datoen 5 år efter denne forordnings ikrafttrædelsesdato*].

3. Den delegation af beføjelser, der er omhandlet i artikel 28, stk. 3, og artikel 38, stk. 2, kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i *Den Europæiske Unions Tidende* eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

4. Inden vedtagelsen af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale om bedre lovgivning af 13. april 2016.

5. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.

6. En delegeret retsakt vedtaget i henhold til artikel 28, stk. 3, og artikel 38, stk. 2, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og til Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har givet Kommissionen meddelelse om, at de ikke agter at gøre indsigelse. Fristen forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.

KAPITEL IX

OVERGANGSBESTEMMELSER OG AFSLUTTENDE BESTEMMELSER

AFDELING I

Artikel 51

Revisionsklausul

Senest den [*EUT: Indsæt datoen 5 år efter denne forordnings ikrafttrædelsesdato*] foretager Kommissionen efter høring af EBA, ESMA, EIOPA og ESRB en gennemgang og forelægger en rapport for Europa-Parlamentet og Rådet, eventuelt ledsaget af et lovgivningsmæssigt forslag til retsakt vedrørende kriterierne for udpegelse af kritiske tredjepartsudbydere af IKT-tjenester i henhold til artikel 28, stk. 2.

AFDELING II

ÆNDRINGER

Artikel 52

Ændring af forordning (EF) nr. 1060/2009

Bilag I, afsnit A, punkt 4, første afsnit, i forordning (EF) nr. 1060/2009 affattes således:

> "Et kreditvurderingsbureau skal have passende administrative og regnskabsmæssige procedurer, interne kontrolmekanismer, effektive procedurer til risikovurdering og effektive kontrol- og sikkerhedsforanstaltninger med henblik på styring af sine IKT-systemer og i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2021/xx [DORA]*.
>
> * Europa-Parlamentets og Rådets forordning (EU) 2021/xx [...] (EUT L XX af DD.MM.ÅÅÅÅ, s. X)."

Artikel 53

Ændringer af forordning (EU) nr. 648/2012

I forordning (EU) nr. 648/2012 foretages følgende ændringer:

1) Artikel 26 ændres således:

a) Stk. 3 affattes således:

"3. En CCP opretholder og anvender en sådan organisatorisk struktur, som er nødvendig til at sikre kontinuitet og regelmæssighed i leveringen af dens tjenesteydelser og udøvelsen af dens aktiviteter. Den anvender med henblik herpå hensigtsmæssige og forholdsmæssigt afpassede systemer, ressourcer og procedurer, herunder IKT-systemer, som styres i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2021/xx [DORA]*.

* Europa-Parlamentets og Rådets forordning (EU) 2021/xx [...] (EUT L XX af DD.MM.ÅÅÅÅ, s. X)."

b) Stk. 6 udgår.

2) Artikel 34 ændres således:

a) Stk. 1 affattes således:

"1. En CCP udarbejder, gennemfører og opretholder en passende forretningskontinuitetsplan og en katastrofeberedskabsplan, som omfatter planer for IKT-driftsstabilitet og IKT-katastrofeberedskabsplaner, der er udarbejdet i overensstemmelse med forordning (EU) 2021/xx [DORA], og som har til formål at beskytte dens funktioner, sikre rettidig genopretning af transaktioner og opfyldelse af CCP'ens forpligtelser."

b) Stk. 3, første afsnit, affattes således:

"For at sikre ensartet anvendelse af denne artikel udarbejder ESMA efter høring af medlemmerne af ESCB udkast til reguleringsmæssige tekniske standarder, der præciserer de elementer og krav, som forretningskontinuitetspolitikken og katastrofeberedskabsplanen mindst skal indeholde, eksklusive planer for IKT-driftsstabilitet og IKT-katastrofeberedskabsplaner."

3) Artikel 56, stk. 3, første afsnit, affattes således:

"3. For at sikre den ensartede anvendelse af denne artikel udarbejder ESMA udkast til reguleringsmæssige tekniske standarder, som præciserer oplysningerne i ansøgningen om registrering, jf. stk. 1, litra a), dog ikke oplysningerne om krav til IKT-risikostyring."

4) Artikel 79, stk. 1 og 2, affattes således:

"1. Et transaktionsregister skal identificere kilderne til operationelle risici og desuden reducere dem ved at udvikle passende systemer, kontroller og procedurer, herunder IKT-systemer, der styres i overensstemmelse med forordning (EU) 2021/xx [*DORA*].

2. Et transaktionsregister udarbejder, gennemfører og opretholder en hensigtsmæssig forretningskontinuitetsplan og en katastrofeberedskabsplan, herunder planer for IKT-driftsstabilitet og

IKT-katastrofeberedskabsplaner, som er udarbejdet i overensstemmelse med forordning (EU) 2021/xx [*DORA*], og som har til formål at sikre opretholdelsen af registrets funktioner og sikre rettidig genopretning af transaktioner og opfyldelse af transaktionsregistrets forpligtelser."

5) Artikel 80, stk. 1, udgår.

Artikel 54

Ændringer af forordning (EU) nr. 909/2014

I artikel 45 i forordning (EU) nr. 909/2014 foretages følgende ændringer:

1) Stk. 1 affattes således:

2) CSD'er skal identificere kilder til operationelle risici, både interne og eksterne, og ligeledes begrænse deres indvirkning ved at anvende passende IT-værktøjer, kontroller og procedurer, som er oprettet og styres i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2021/xx [*DORA*]*, samt ved anvende eventuelle andre relevante værktøjer, kontroller og procedurer for andre typer af operationelle risici, herunder for alle de værdipapirafviklingssystemer, som de driver.

3) Europa-Parlamentets og Rådets forordning (EU) 2021/xx [...] (EUT L XX af DD.MM.ÅÅÅÅ, s. X)."

4) Stk. 2 udgår.

5) Stk. 3 og 4 affattes således:

"3. CSD'er udarbejder, gennemfører og opretholder for tjenesteydelser, som de leverer, samt for hvert af de værdipapirafviklingssystemer, som de driver, en passende forretningskontinuitetspolitik og en katastrofeberedskabsplan, herunder planer for IKT-driftsstabilitet og IKT-katastrofeberedskabsplaner, som er udarbejdet i overensstemmelse med forordning (EU) 2021/xx [*DORA*], og som har til formål at sikre beskyttelse af deres tjenesteydelser, rettidig genopretning af transaktioner og opfyldelse af deres forpligtelser i tilfælde af hændelser, som i høj grad risikerer at afbryde transaktioner.

4. Planerne i stk. 3 skal give mulighed for at genoptage alle transaktioner og deltageres positioner fra det tidspunkt, hvor de blev afbrudt, for at give deltagerne i en CSD mulighed for at opretholde driftssikkerheden og foretage afvikling på den planlagte dato, bl.a. ved at sikre, at kritiske IT-systemer kan genoptage driften fra det tidspunkt, hvor de blev afbrudt som fastsat i artikel 11, stk. 5 og 7, i forordning (EU) 2021/xx [*DORA*]."

6) Stk. 6, første afsnit, affattes således:

CSD'er identificerer, overvåger og forvalter de risici, som de vigtigste deltagere i de værdipapirafviklingssystemer, de driver, samt serviceydere og andre CSD'er eller andre markedsinfrastrukturer kan indebære for deres transaktioner. De giver efter anmodning de kompetente og relevante myndigheder oplysninger om sådanne risici,

der identificeres. De underretter også omgående den kompetente myndighed og relevante myndigheder om eventuelle operationelle hændelser som følge af sådanne risici, dog ikke om IKT-risici."

7) Stk. 7, første afsnit, affattes således:

"ESMA udarbejder i tæt samarbejde med medlemmerne af ESCB udkast til reguleringsmæssige tekniske standarder med henblik på at præcisere de operationelle risici i stk. 1 og 6, med undtagelse af IKT-risici, og metoderne til at teste, håndtere eller begrænse de pågældende risici, herunder forretningskontinuitetspolitikkerne og katastrofeberedskabsplanerne i stk. 3 og 4 og metoderne til vurdering deraf."

Artikel 55

Ændringer af forordning (EU) nr. 600/2014

I forordning (EU) nr. 600/2014 foretages følgende ændringer:

1) Artikel 27g ændres således:

a) Stk. 4 udgår.

b) Stk. 8, litra c), affattes således:

c) "c) de konkrete organisatoriske krav, der er fastsat i stk. 3 og 5."

2) Artikel 27h ændres således:

a) Stk. 5 udgår.

b) Stk. 8, litra e), affattes således:

"e) de konkrete organisatoriske krav, der er fastsat i stk. 4."

3) Artikel 27i ændres således:

a) Stk. 3 udgår.

b) Stk. 5, litra b) affattes således:

"b) de konkrete organisatoriske krav, der er fastsat i stk. 2 og 4."

Artikel 56

Ikrafttræden og anvendelse

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Den anvendes fra den [*Publikationskontoret: Indsæt dato — 12 måneder efter ikrafttrædelsesdatoen*].

Dog finder artikel 23 og 24 anvendelse fra den [*Indsæt datoen — 36 måneder efter denne forordnings ikrafttrædelsesdato*].

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den […].

På Europa-Parlamentets vegne	*På Rådets vegne*
Formand	*Formand*

FINANSIERINGSOVERSIGT

1. FORSLAGETS/INITIATIVETS RAMME

1.1. Forslagets/initiativets betegnelse

1.2. Berørt(e) politikområde(r)

1.3. Forslagets/initiativets art

1.4. Mål

1.5. Forslagets/initiativets begrundelse

1.6. Forslagets/initiativets varighed og finansielle virkninger

1.7. Påtænkt(e) forvaltningsmetode(r)

2. FORVALTNINGSFORANSTALTNINGER

2.1. Bestemmelser om kontrol og rapportering

2.2. Forvaltnings- og kontrolsystem(er)

2.3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3.1. Berørt(e) udgiftspost(er) på budgettet og udgiftsområde(r) i den flerårige finansielle ramme

3.2. Anslåede virkninger for udgifterne

3.2.1. Sammenfatning af de anslåede virkninger for udgifterne

3.2.2. Anslåede virkninger for bevillingerne

3.2.3. Anslåede virkninger for administrationsbevillingerne

3.2.4. Forenelighed med indeværende flerårige finansielle ramme

3.2.5. Tredjemands bidrag til finansieringen

3.3. Anslåede virkninger for indtægterne

Bilag

Generelle antagelser

Tilsynsbeføjelser

FINANSIERINGSOVERSIGT — "AGENTURER"

1. FORSLAGETS/INITIATIVETS RAMME

1.1. Forslagets/initiativets betegnelse

Forslag til Europa-Parlamentets og Rådets forordning om digital operationel modstandsdygtighed i den finansielle sektor.

1.2. Berørt(e) politikområde(r)

Politikområde: Finansiel stabilitet, finansielle tjenesteydelser og kapitalmarkedsunionen Aktivitet: Digital operationel modstandsdygtighed

1.3. Forslaget vedrører

☑ en ny foranstaltning

☐ en ny foranstaltning som opfølgning på et pilotprojekt/en forberedende foranstaltning[50]

☐ en forlængelse af en eksisterende foranstaltning

☐ en sammenlægning af en eller flere foranstaltninger til en anden/en ny foranstaltning

1.4. Mål

1.4.1. Overordnet mål

Det overordnede mål med initiativet er at styrke den digitale operationelle modstandsdygtighed i enheder i EU's finansielle sektor ved at strømline og ajourføre eksisterende regler og indføre nye krav, hvor der er huller. Dette vil også styrke det fælles regelsæt i forhold til dets digitale dimension. Det overordnede mål kan inddeles i tre generelle målsætninger: 1) mindske risikoen for finansielle forstyrrelser og ustabilitet, 2) mindske den administrative byrde og øge den tilsynsmæssige effektivitet, og 3) øge forbrugerbeskyttelsen og investorbeskyttelsen.

1.4.2. Specifikke mål

[50] Jf. finansforordningens artikel 58, stk. 2, litra a) hhv. b).

Forslaget har følgende specifikke mål:

En mere grundig håndtering af risici forbundet med informations- og kommunikationsteknologier ("IKT") og styrkelse af den generelle digitale modstandsdygtighed i den finansielle sektor.

Strømlining af indberetningen IKT-relaterede hændelser og håndtering af overlappende indberetningskrav.

Finansielle tilsynsmyndigheders mulighed for at få adgang til oplysninger om IKT-relaterede hændelser.

Sikring af, at de finansielle enheder, der er omfattet af dette forslag, vurderer effektiviteten af deres forebyggende foranstaltninger og foranstaltninger vedrørende modstandsdygtighed og identificerer IKT-relaterede sårbarheder.

Begrænsning af fragmenteringen på det indre marked og muliggørelse af grænseoverskridende accept af testresultater.

Styrkelse af de kontraktlige sikkerhedsforanstaltninger for finansielle enheder, der anvender IKT-tjenester, herunder for regler om outsourcing (tilsyn med tredjepartsudbydere af IKT-tjenester) (i det følgende benævnt "TPP'er")).

Muliggørelse af tilsyn med de aktiviteter, der udføres af kritiske IKT-TPP'er.

Tilskyndelse til udveksling af trusselsefterretninger i den finansielle sektor.

1.4.3. Forventede resultater og virkninger

Angiv, hvilke virkninger forslaget/initiativet forventes at få for modtagerne/målgruppen.

En lov om digital operationel modstandsdygtighed i den finansielle sektor vil sikre en omfattende ramme, der inddrager alle aspekter af digital operationel modstandsdygtighed, og vil være effektiv med hensyn til at forbedre den overordnede operationelle modstandsdygtighed i den finansielle sektor. Den vil sikre klarhed og sammenhæng inden for det fælles regelsæt.

Det vil også gøre samspillet med NIS-direktivet og revisionen heraf klarere og mere sammenhængende. Det vil skabe klarhed for finansielle enheder om de forskellige regler om digital operationel modstandsdygtighed, som de skal overholde, navnlig for så vidt angår de finansielle enheder, der har flere tilladelser og har aktiviteter på forskellige markeder i EU.

1.4.4. Resultatindikatorer

Angiv indikatorerne for overvågning af fremskridt og resultater.

Mulige indikatorer:

Antal IKT-relaterede hændelser i EU's finansielle sektor og deres virkninger

Antal større IKT-relaterede hændelser, der er indberettet til tilsynsmyndighederne

Antal finansielle enheder, der vil være forpligtet til at udføre trusselsbaserede penetrationstest ("TLPT")

Antal finansielle enheder, der anvender standardkontraktbestemmelser, når de indgår kontraktlige ordningerne med IKT-TPP'er

Antal kritiske IKT-TPP'er, som ESA'erne/tilsynsmyndighederne fører tilsyn med

Antal finansielle enheder, der deltager i ordninger for udveksling af efterretninger

Antal myndigheder, der skal modtage indberetninger om samme IKT-relaterede hændelse

Antal grænseoverskridende TLPT'er

1.5. Forslagets/initiativets begrundelse

1.5.1. Behov, der skal opfyldes på kort eller lang sigt, herunder en detaljeret tidsplan for iværksættelsen af initiativet

Den finansielle sektor afhænger i vid udstrækning af informations- og kommunikationsteknologier (IKT). Til trods for de betydelige fremskridt, der er gjort gennem målrettede politiske og lovgivningsmæssige initiativer på nationalt plan og EU-plan, udgør IKT-risici fortsat en udfordring for den operationelle modstandsdygtighed, kapaciteten og stabiliteten i EU's finansielle system. Den reform, der fulgte efter den finansielle krise i 2008 styrkede primært den finansielle modstandsdygtighed i EU's finansielle sektor og sigtede mod

at bevare EU's konkurrenceevne og stabilitet set fra et økonomisk, tilsyns- og markedsadfærdsmæssigt perspektiv. IKT-sikkerhed og overordnet digital modstandsdygtighed udgør dele af den operationelle risiko, men der har været minde fokus herpå i den lovgivningsmæssige dagsorden efter krisen, og de er kun blevet udviklet på nogle områder af EU's politik for og regulering af de finansielle markeder, eller kun i nogle få medlemsstater. Dette udmønter sig i følgende udfordringer, som bør afhjælpes med dette forslag:

Den EU-lovramme, der dækker IKT-risici og operationel modstandsdygtighed i den finansielle sektor, er fragmenteret og ikke helt konsekvent.

Manglen på ensartede krav til indberetning af IKT-relaterede hændelser, gør at tilsynsmyndighederne har et ufuldstændigt overblik over karakteren, hyppigheden, væsentligheden og virkningerne af hændelser.

Nogle finansielle enheder står over for komplekse, overlappende og potentielt inkonsekvente krav til indberetning for samme IKT-relaterede hændelse.

Utilstrækkelig udveksling af oplysninger og utilstrækkeligt samarbejde om efterretninger om cybertrusler på et strategisk, taktisk og operationelt plan forhindrer, at individuelle finansielle enheder i tilstrækkelig grad kan vurdere, overvåge, forsvare sig mod og sætte ind over for cybertrusler.

I nogle finansielle delsektorer kan der være mange og ukoordinerede rammer for penetrationstest og afprøvning af modstandsdygtighed, kombineret med manglende grænseoverskridende anerkendelse af resultater, mens andre delsektorer ikke har sådanne afprøvningsrammer.

Manglen på tilsynsmæssig indsigt i de aktiviteter, der udføres af finansielle enheder, og som leveres af IKT-TTP'er, eksponerer finansielle enheder individuelt og det finansielle system som helhed for operationelle risici.

Finansielle tilsynsmyndigheder hverken udstyret med et tilstrækkeligt mandat eller værktøjerne til at overvåge og styre koncentrationsrisici og systemiske risici, der forårsages af finansielle enheders afhængighed af IKT-tredjeparter.

1.5.2. Merværdien ved en indsats fra EU's side (f.eks. koordineringsfordele, retssikkerhed, større effektivitet eller komplementaritet). Ved "merværdien ved en indsats fra EU's side" forstås her merværdien af EU's intervention i forhold til den værdi, som medlemsstaterne ville have skabt enkeltvist.

Begrundelse for en indsats på EU-plan (forudgående):

Digital operationel modstandsdygtighed er et spørgsmål af fælles interesse for EU's finansielle markeder. En indsats på EU-plan vil give flere fordele og en større værdi end de separate foranstaltninger, der træffes på nationalt plan. Hvis disse operationelle bestemmelser om IKT-risici ikke tilføjes, ville det fælles regelsæt rigtig indeholde redskaberne til at håndtere alle andre former for risici på europæisk plan, men det ville udelade aspekter vedrørende digital operationel modstandsdygtighed eller lade dem omfatte af fragmenterede og ukoordinerede initiativer på nationalt plan. Dette forslag vil skabe juridisk klarhed om, hvorvidt og hvordan bestemmelser om digital operationel modstandsdygtighed finder anvendelse, navnlig for

grænseoverskridende finansielle enheder, og det vil fjerne behovet for, at medlemsstaterne individuelt forbedrer regler, standarder og forventninger vedrørende operationel modstandsdygtighed og cybersikkerhed som indsats mod EU-reglernes nuværende begrænsede anvendelsesområde og NIS-direktivets generelle karakter.

Forventet merværdi på EU-plan (efterfølgende):

Unionens indsats vil i væsentlig grad øge politikkens effektivitet og samtidig mindske kompleksiteten og lette den finansielle og administrative byrde, der pålægges alle finansielle enheder. Det vil harmonisere et område af økonomien med så tæt indbyrdes forbundethed, som er så dybt integreret, og som allerede høster fordelene ved et enkelt regelsæt og tilsyn. Hvad angår indberetning af IKT-relaterede hændelser, vil forslaget mindske indberetningsbyrden — og de implicitte omkostninger — i forbindelse med indberetning af samme IKT-relaterede hændelse til forskellige EU-myndigheder og/eller nationale myndigheder. Det vil også lette den gensidige anerkendelse/accept af testresultaterne for enheder, der har aktiviteter på tværs af grænserne, og som er omfattet af flere afprøvningsrammer i forskellige medlemsstater.

1.5.3. Erfaringer fra lignende foranstaltninger

Nyt initiativ

1.5.4. Sammenhæng med den flerårige finansielle ramme og eventuelle synergivirkninger med andre relevante instrumenter

Formålet med dette forslag er i overensstemmelse med en række andre EU-politikker og igangværende initiativer, navnlig direktivet om cybersikkerhed (NIS-direktivet) og direktivet om europæisk kritisk infrastruktur. Forslaget vil bevare de fordele, der er forbundet med den horisontale ramme for cybersikkerhed, ved fortsat at lade de tre finansielle delsektorer indgå i NIS-direktivets anvendelsesområde. Ved fortsat at være tilknyttet økosystemet under NIS-direktivet vil finansielle tilsynsmyndigheder kunne udveksle relevante oplysninger med NIS-myndigheder og deltage i NIS-samarbejdsgruppen. Forslaget vil ikke have indvirkning på NIS-direktivet, men snarere bygge videre på direktivet og afhjælpe mulige overlapninger ved hjælp af en undtagelse, der bygger på en særlig lovregel. Samspillet mellem forordningen om finansielle tjenesteydelser og NIS-direktivet vil fortsat være omfattet af en klausul, der bygger på en særlig lovregel, hvorved finansielle enheder fritages fra væsentlige krav i NIS-direktivet og der undgås overlapninger mellem de to retsakter. Derudover er forslaget i overensstemmelse med direktivet om europæisk kritisk infrastruktur, som i øjeblikket revideres for at styrke beskyttelsen af og modstandsdygtigheden i kritisk infrastruktur mod ikke-cyberrelaterede trusler.

Dette forslag vil ikke have nogen indvirkning på den flerårige finansielle ramme (FFR). For det første vil tilsynsrammen for kritiske tredjepartsudbydere af IKT-tjenester blive finansieret fuldt ud af gebyrer, der opkræves hos disse udbydere. For det andet varetages de yderligere reguleringsopgaver forbundet med digital operationel robusthed, der er overdraget til ESA'erne, ved intern omfordeling af eksisterende personale.

Dette vil udmønte sig i et forslag om at øge myndighedens autoriserede personale under den fremtidige årlige budgetprocedure. Myndigheden vil fortsat arbejde på at maksimere synergier og effektivitetsgevinster (bl.a. via IT-systemer) og nøje overvåge den ekstra arbejdsbyrde, der er forbundet med dette forslag, hvilket vil blive afspejlet i det niveau af autoriseret personale, som myndigheden har anmodet om i den årlige budgetprocedure.

1.5.5. Vurdering af de forskellige tilgængelige finansieringsmuligheder, herunder muligheden for omfordeling

Flere finansieringsmuligheder blev overvejet:

For det første kan de yderligere omkostninger finansieres gennem ESA'ernes sædvanlige finansieringsmekanisme. Dette vil imidlertid medføre en væsentlig forøgelse af EU's bidrag til ESA'ernes finansielle ressourcer.

Denne mulighed vælges for de omkostninger, der vedrører reguleringsopgaver i forbindelse med dette forslag. ESA'erne vil ganske rigtigt blive anmodet om at omfordele eksisterende personale med henblik på at udvikle en række tekniske standarder. De yderligere omkostninger i forbindelse med tilsynet med kritiske TPP'er kan dog ikke dækkes ved en omfordeling af ressourcer inden for ESA'erne, som også varetager andre opgaver end dem, der er omhandlet i dette forslag, samt i henhold til andre EU-retsakter. Dertil kommer, at de tilsynsopgaverne, der vedrører digital operationel modstandsdygtighed, kræver specifik teknisk viden og ekspertise. Da ESA'ernes nuværende niveau af sådanne ressourcer er utilstrækkeligt, er der behov for yderligere ressourcer.

Endelig vil der ifølge forslaget blive opkrævet gebyrer hos den kritiske IKT-TPP, som er omfattet af tilsynet. Formålet med disse er at dække alle de supplerende ressourcer, som ESA'erne har brug for, således at de varetage deres nye opgaver og udøve deres nye beføjelser.

1.6. Forslagets/initiativets varighed og finansielle virkninger

☐ **Begrænset varighed**

☐ Forslag/initiativ gældende fra [DD/MM]YYYY til [DD/MM]YYYY

☐ Finansielle virkninger fra YYYY til YYYY

☑ **ubegrænset varighed**

Iværksættelse med en indkøringsperiode fra 2021

derefter gennemførelse i fuldt omfang.

1.7. Påtænkt(e) forvaltningsmetode(r)[51]

Direkte forvaltning ved Kommissionen via

☐ gennemførelsesorganer

☐ **Delt forvaltning** i samarbejde med medlemsstaterne

☑ **Indirekte forvaltning** ved at overlade budgetgennemførelsesopgaver til:

☐ internationale organisationer og deres organer (angives nærmere)

☐ Den Europæiske Investeringsbank og Den Europæiske Investeringsfond

☑ de organer, der er omhandlet i finansforordningens artikel 70 og 71

☐ offentligretlige organer

☐ privatretlige organer, der har fået overdraget samfundsopgaver, forudsat at de stiller tilstrækkelige finansielle garantier

☐ privatretlige organer, undergivet lovgivningen i en medlemsstat, som har fået overdraget gennemførelsen af et offentlig-privat partnerskab, og som stiller tilstrækkelige finansielle garantier

☐ personer, der har fået overdraget gennemførelsen af specifikke aktioner i den fælles udenrigs- og sikkerhedspolitik i henhold til afsnit V i traktaten om Den Europæiske Union, og som er udpeget i den relevante basisretsakt.

[51] Forklaringer vedrørende forvaltningsmetoder og henvisninger til finansforordningen findes på webstedet BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Bemærkninger

Ikke relevant.

2. FORVALTNINGSFORANSTALTNINGER

2.1. Bestemmelser om kontrol og rapportering

Angiv hyppighed og betingelser.

I overensstemmelse med allerede eksisterende ordninger udarbejder ESA'erne regelmæssige rapporter om deres aktiviteter (herunder intern rapportering til øverste ledelse, rapportering til organer og udarbejdelse af årsberetning) og er underlagt revision ved Revisionsretten og Kommissionens interne revisionstjeneste om deres forbrug af ressourcer og resultater. Overvågning og rapportering af de tiltag, der er omfattet af forslaget, vil være i overensstemmelse med allerede eksisterende krav samt eventuelle nye krav som følge af dette forslag.

2.2. Forvaltnings- og kontrolsystem(er)

2.2.1. Begrundelse for den/de påtænkte forvaltningsmetode(r), finansieringsmekanisme(r), betalingsvilkår og kontrolstrategi

Forvaltningen vil blive varetaget indirekte gennem ESA'erne. Finansieringsmekanismen vil blive gennemført ved hjælp af gebyrer, der opkræves hos de pågældende kritiske IKT-TPP'er.

2.2.2. Oplysninger om de udpegede risici og det/de interne kontrolsystem(er), der etableres for at afbøde dem

For så vidt angår den retlige, økonomisk forsvarlige og effektive anvendelse af de bevillinger, der følger af forslaget, forventes det, at forslaget ikke medfører nye væsentlige risici, som ikke allerede er omfattet af eksisterende interne kontrolordninger. Sikring af rettidig opkrævning af gebyrer hos de pågældende kritiske IKT-TPP'er kan derimod udgøre en ny udfordring.

2.2.3. Vurdering af og begrundelse for kontrolforanstaltningernes omkostningseffektivitet (forholdet mellem kontrolomkostningerne og værdien af de forvaltede midler) samt vurdering af den forventede risiko for fejl (ved betaling og ved afslutning)

Der er allerede indført forvaltnings- og kontrolsystemer i overensstemmelse med ESA-forordningerne. ESA'erne arbejder tæt sammen med Kommissionens interne revisionstjeneste for at sikre, at de relevante standarder overholdes inden for alle områder af det interne kontrolsystem. Disse ordninger vil også gælde i forhold til ESA'ernes rolle i henhold til det foreliggende forslag. Dertil kommer, at Europa-Parlamentet hvert regnskabsår, efter henstilling fra Rådet, meddeler decharge til hver ESA for gennemførelsen af dens budgetter.

2.3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

Angiv eksisterende eller påtænkte forebyggelses- og beskyttelsesforanstaltninger, f.eks. fra strategien til bekæmpelse af svig.

Med henblik på bekæmpelse af svig, bestikkelse og anden ulovlig aktivitet finder bestemmelserne i Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 883/2013 af 11. september 2013 om undersøgelser, der foretages af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF), anvendelse på ESA'erne uden nogen begrænsninger.

ESA'erne har en særskilt strategi til bekæmpelse af svig og en deraf følgende handlingsplan. ESA'ernes styrkede foranstaltninger til bekæmpelse af svig stemmer overens med regler og retningslinjer i henhold til finansforordningen (foranstaltninger mod svig som led i forsvarlig finansiel forvaltning), OLAF's politik for forebyggelse af svig, Kommissionens strategi til bekæmpelse af svig (COM(2011) 376) samt den fælles tilgang til EU's decentraliserede agenturer (juli 2012) og den tilhørende køreplan.

Endvidere indeholder forordningerne om oprettelse af ESA'erne såvel som ESA'erne finansforordning bestemmelser om gennemførelse og kontrol af ESA'ernes budgetter og gældende finansielle regler, herunder dem, der vedrører bekæmpelse af svig og uregelmæssigheder.

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3.1. Berørt(e) udgiftspost(er) på budgettet og udgiftsområde(r) i den flerårige finansielle ramme

Eksisterende udgiftsposter på budgettet

I samme rækkefølge som udgiftsområderne i den flerårige finansielle ramme og budgetposterne.

Udgiftsområde i den flerårige finansielle ramme	Budgetpost	Udgifternes art	Bidrag			
	Nummer	OB/IOB[52]	fra EFTA-lande[53]	fra kandidatlande[54]	fra tredjelande	i henhold til finansforordningens artikel 21, stk. 2, litra b)

Nye budgetposter, som der er søgt om.

I samme rækkefølge som udgiftsområderne i den flerårige finansielle ramme og budgetposterne.

52 OB = opdelte bevillinger/IOB = ikke-opdelte bevillinger.

53 EFTA: Den Europæiske Frihandelssammenslutning.

54 Kandidatlande og, efter omstændighederne, potentielle kandidater på Vestbalkan

Udgiftsområde i den flerårige finansielle ramme	Budgetpost	Udgifternes art	Bidrag			
	Nummer	OB/IOB	fra EFTA-lande	fra kandidatlande	fra tredjelande	i henhold til finansforordningens artikel 21, stk. 2, litra b)

3.2. Anslåede virkninger for udgifterne

3.3. Sammenfatning af de anslåede virkninger for udgifterne

i mio. EUR (tre decimaler)

Udgiftsområde i den flerårige finansielle ramme	Nummer	Udgiftsområde

GD: <..>			2020	2021	2022	2023	2024	2025	2026	2027	**I ALT**
	Forpligtelser	1.									
	Betalinger	2.									
Bevillinger I ALT til GD [...]	Forpligtelser										
	Betalinger										

Udgiftsområde i den flerårige finansielle ramme		

i mio. EUR (tre decimaler)

		2022	2023	2024	2025	2026	2027	**I ALT**
GD'er:								
• Menneskelige ressourcer								
• Andre administrationsudgifter								
I ALT GD'er	Bevillinger							

Bevillinger I ALT under UDGIFTSOMRÅDE […] i den flerårige finansielle ramme	(Forpligtelser i alt = betalinger i alt)							

i mio. EUR (3 decimaler) i faste priser

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**I ALT**
Bevillinger I ALT under UDGIFTSOMRÅDE 1 i den flerårige finansielle ramme	Forpligtelser							
	Betalinger							

3.3.1. Anslåede virkninger for bevillingerne

☑ Forslaget/initiativet medfører ikke anvendelse af aktionsbevillinger

☐ Forslaget/initiativet medfører anvendelse af aktionsbevillinger som anført herunder:

Forpligtelsesbevillinger i mio. EUR (3 decimaler) i faste priser

Der angives mål og resultater ⇩			2022		2023		2024		2025		2026		2027		**I ALT**	
	RESULTATER															
	Type[55]	Resultatemes gnsntl. omkostning	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal resultater i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 1[56] ...																
- Resultat																
Subtotal for specifikt mål nr. 1																
SPECIFIKT MÅL NR. 2																
- Resultat																
Subtotal for specifikt mål nr. 2																
OMKOSTNINGER I ALT																

55 Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

56 Som beskrevet i punkt 1.4.2. "Specifikke mål ...".

3.3.2. Anslåede virkninger for administrationsbevillingerne

3.3.2.1. Resumé

☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

☑ Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (3 decimaler) i faste priser

EBA, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**I ALT**
Midlertidigt ansatte (AD)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Midlertidigt ansatte (AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Kontraktansatte							
Udstationerede nationale eksperter							
I ALT	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Personalebehov (i årsværk):

EBA, EIOPA, ESMA & EØS	2022	2023	2024	2025	2026	2027	**I ALT**
Midlertidigt ansatte (AD) EBA=5, EIOPA=5, ESMA=5	15	15	15	15	15	15	15
Midlertidigt ansatte (AST) EBA=1, EIOPA=1, ESMA=1	3	3	3	3	3	3	3
Kontraktansatte							
Udstationerede nationale eksperter							
I ALT	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Anslået behov for menneskelige ressourcer i (de overordnede) generaldirektorater

☑ Forslaget/initiativet medfører ikke anvendelse af menneskelige ressourcer

☐ Forslaget/initiativet medfører anvendelse af menneskelige ressourcer som anført herunder:

Overslag angives i hele tal (eller med højst én decimal)

		2022	2023	2024	2025	2026	2027
• **Stillinger i stillingsfortegnelsen (tjenestemænd og midlertidigt ansatte)**							
• **Eksternt personale (i årsværk: FTÆ)**[57]							
XX 01 02 01 (KA, UNE, V under den samlede bevillingsramme)							
XX 01 02 02 (KA, LA, UNE, V og JED i delegationerne)							
XX 01 04 ***yy***[58]	- i hovedsædet[59]						
	- i delegationer						
XX 01 05 02 (KA, UNE, V — indirekte forskning)							
10 01 05 02 (KA, UNE, V – direkte forskning)							
Andre budgetposter (skal angives)							
I ALT							

XX angiver det berørte politikområde eller budgetafsnit.

Personalebehovet vil blive dækket ved hjælp af det personale, som generaldirektoratet allerede har afsat til aktionen, og/eller interne rokader i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

Opgavebeskrivelse:

Tjenestemænd og midlertidigt ansatte	
Eksternt personale	

[57] KA = kontraktansatte, LA: lokalt ansatte, UNE: udstationerede nationale eksperter, V: vikarer, JED = junioreksperter ved delegationerne.

[58] Delloft for eksternt personale under aktionsbevillingerne (tidligere BA-poster).

[59] Angår især strukturfondene, Den Europæiske Landbrugsfond for Udvikling af Landdistrikterne (ELFUL) og Den Europæiske Fiskerifond (EFF).

Beskrivelsen af, hvordan udgifterne til fuldtidsækvivalenterne er beregnet, bør medtages i afsnit 3 i bilag V.

3.3.3. Forenelighed med indeværende flerårige finansielle ramme

☑ Forslaget/initiativet er foreneligt med indeværende flerårige finansielle ramme

☐ Forslaget/initiativet kræver omlægning af det relevante udgiftsområde i den flerårige finansielle ramme

☐ Forslaget/initiativet kræver, at fleksibilitetsinstrumentet anvendes, eller at den flerårige finansielle ramme revideres[60].

Der redegøres for behovet med angivelse af de berørte udgiftsområder og budgetposter og beløbenes størrelse […]

3.3.4. Tredjemands bidrag til finansieringen

☐ Forslaget/initiativet indeholder ikke bestemmelser om samfinansiering med tredjepart.

☑ Forslaget/initiativet indeholder bestemmelser om samfinansiering, jf. følgende overslag:

i mio. EUR (tre decimaler)

EBA

	2022	2023	2024	2025	2026	2027	I alt
Omkostningerne dækkes 100 % af gebyrer, der opkræves hos de enheder, der føres tilsyn med.[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Samfinansierede bevillinger I ALT	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	I alt
Omkostningerne dækkes 100 % af gebyrer, der opkræves hos de enheder, der føres tilsyn med.[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560

60 Jf. artikel 11 og 17 i Rådets forordning (EU, Euratom) nr. 1311/2013 om fastlæggelse af den flerårige finansielle ramme for årene 2014-2020.

61 100 % af de samlede anslåede omkostninger plus arbejdsgiverens fulde pensionsbidrag

62 100 % af de samlede anslåede omkostninger plus arbejdsgiverens fulde pensionsbidrag

Samfinansierede bevillinger I ALT	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	I alt
Omkostningerne dækkes 100 % af gebyrer, der opkræves hos de enheder, der føres tilsyn med.[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Samfinansierede bevillinger I ALT	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Anslåede virkninger for indtægterne

☑ Forslaget/initiativet har ingen finansielle virkninger for indtægterne

☐ Forslaget/initiativet har følgende finansielle virkninger:

☐ for egne indtægter

☐ for andre indtægter

☐ Angiv, om indtægterne er formålsbestemte

i mio. EUR (tre decimaler)

Indtægtspost på budgettet:	Bevillinger til rådighed i indeværende regnskabsår	Forslagets/initiativets virkninger[64]						
		År **n**	År **n + 1**	År **n + 2**	År **n + 3**	Der indsættes flere år, hvis virkningerne varer længere (jf. punkt 1.6)		
Artikel…								

For diverse indtægter, der er formålsbestemte, angives det, hvilke af budgettets udgiftsposter der påvirkes.

[…]

Det oplyses, hvilken metode der er benyttet til at beregne virkningerne for indtægterne.

[…]

63 100 % af de samlede anslåede omkostninger plus arbejdsgiverens fulde pensionsbidrag

64 Med hensyn til EU's traditionelle egne indtægter (told og sukkerafgifter) opgives beløbene netto, dvs. bruttobeløb, hvorfra der er trukket opkrævningsomkostninger på 20 %.

BILAG

Generelle antagelser

Afsnit I - Personaleudgifter

Følgende specifikke antagelser er anvendt ved beregningen af personaleudgifterne på grundlag af de konstaterede personalebehov, som der redegøres for nedenfor:

- Det ekstra personale, der ansættes i 2022, budgetteres med i 6 måneder på grund af den tid, det tager at ansætte det ekstra personale
- Den gennemsnitlige årlige udgift til en midlertidigt ansat er 150 000 EUR, heraf 25 000 EUR i "habillage"-omkostninger (bygninger, IT osv.).
- Den justeringskoefficient, der anvendes på personalelønninger i Paris (EBA og ESMA og Frankfurt (EIOPA), er henholdsvis 117.7 og 99.4.
- Arbejdsgiverbidragene for midlertidigt ansatte er baseret på de almindelige grundlønninger, der indgår i de gennemsnitlige årlige udgifter, dvs. 95 660 EUR
- De yderligere midlertidigt ansatte er AD5 og AST.

Afsnit II - Infrastruktur- og driftsudgifter

Omkostningerne beregnes ved at multiplicere antallet af ansatte med den andel af året, hvor der anvendes standardomkostninger til "habillage", dvs. 25 000 EUR.

Afsnit III -Aktionsudgifter

Omkostningerne vurderes på grundlag af følgende antagelser:

- Oversættelsesomkostningerne fastsættes til 350 000 EUR pr. år for hver af ESA'erne.
- Engangsomkostningerne til IT på 500 000 EUR pr. ESA antages at blive afholdt i løbet af de to år 2022 og 2023 på grundlag af en opdeling på halvdelen hvert år. De årlige vedligeholdelsesomkostninger fra 2024 pr. ESA anslås til 50 000 EUR.
- De årlige omkostninger til tilsyn på stedet anslås til 200 000 EUR pr. ESA.

De ovenfor anførte skøn resulterer i følgende omkostninger pr. år:

Udgiftsområde i den flerårige finansielle ramme	Nummer	

Faste priser

EBA:			2022	2023	2024	2025	2026	2027	**I ALT**
Afsnit 1:	Forpligtelser	1.	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Betalinger	2.	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Afsnit 2:	Forpligtelser	1a.	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Betalinger	2a.	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Afsnit 3:	Forpligtelser	3a.	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Betalinger	3b.	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Bevillinger I ALT til EBA	Forpligtelser	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Betalinger	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022	2023	2024	2025	2026	2027	**I ALT**
Afsnit 1:	Forpligtelser	1.	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Betalinger	2.	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Afsnit 2:	Forpligtelser	1a.	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Betalinger	2a.	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Afsnit 3:	Forpligtelser	3a.	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Betalinger	3b.	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Bevillinger I ALT	Forpligtelser	=1+1a +3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560

til EIOPA	Betalinger	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022	2023	2024	2025	2026	2027	**I ALT**
Afsnit 1:	Forpligtelser	1.	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Betalinger	2.	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Afsnit 2:	Forpligtelser	1a.	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Betalinger	2a.	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Afsnit 3:	Forpligtelser	3a.	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Betalinger	3b.	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Bevillinger I ALT til ESMA	Forpligtelser	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Betalinger	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Forslaget medfører anvendelse af aktionsbevillinger som anført herunder:

Forpligtelsesbevillinger i mio. EUR (3 decimaler) i faste priser

EBA

Der angives mål og resultater ⇩			2022		2023		2024		2025		2026		2027			
	RESULTATER															
	Type[65]	Resultaternes gnsntl. omkostning	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal resultater i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 1[66] Direkte tilsyn med kritiske IKT-TPP'er																
- Resultat				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal for specifikt mål nr. 1																
SPECIFIKT MÅL NR. 2																
- Resultat																
Subtotal for specifikt mål nr. 2																
OMKOSTNINGER I ALT				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Der angives mål og resultater ⇩			2022		2023		2024		2025		2026		2027			
	RESULTATER															
	Type[67]	Resultaternes gnsntl. omkostning	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal resultater i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 1[68] Direkte tilsyn med kritiske IKT-TPP'er																

[65] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

[66] Som beskrevet i punkt 1.4.2. "Specifikke mål ...".

[67] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

[68] Som beskrevet i punkt 1.4.2. "Specifikke mål ...".

- Resultat				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal for specifikt mål nr. 1																
SPECIFIKT MÅL NR. 2																
- Resultat																
Subtotal for specifikt mål nr. 2																
OMKOSTNINGER I ALT				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Der angives mål og resultater ⇩			2022		2023		2024		2025		2026		2027			
	RESULTATER															
	Type[69]	Resultaternes gnsntl. omkostning	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal resultater i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 1[70] Direkte tilsyn med kritiske IKT-TPP'er																
- Resultat				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal for specifikt mål nr. 1																
SPECIFIKT MÅL NR. 2																
- Resultat																
Subtotal for specifikt mål nr. 2																
OMKOSTNINGER I ALT				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

[70] Som beskrevet i punkt 1.4.2. "Specifikke mål ...".

Tilsynsaktiviteterne finansieres fuldt ud af gebyrer, der opkræves hos de enheder, der føres tilsyn med, som følger:

EBA

	2022	2023	2024	2025	2026	2027	I alt
Omkostningerne dækkes 100 % af gebyrer, der opkræves hos de enheder, der føres tilsyn med.[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Samfinansierede bevillinger I ALT	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	I alt
Omkostningerne dækkes 100 % af gebyrer, der opkræves hos de enheder, der føres tilsyn med.[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
Samfinansierede bevillinger I ALT	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	I alt
Omkostningerne dækkes 100 % af gebyrer, der opkræves hos de enheder, der føres tilsyn med.[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Samfinansierede bevillinger I ALT	1,373	1,948	1,748	1,748	1,748	1,748	10,313

[71] 100 % af de samlede anslåede omkostninger plus arbejdsgiverens fulde pensionsbidrag
[72] 100 % af de samlede anslåede omkostninger plus arbejdsgiverens fulde pensionsbidrag
[73] 100 % af de samlede anslåede omkostninger plus arbejdsgiverens fulde pensionsbidrag

SPECIFIKKE OPLYSNINGER

Direkte tilsynsbeføjelser

Indledningsvist bemærkes, at enheder, der er underlagt direkte tilsyn af ESMA, bør betale gebyrer til ESMA (engangsomkostninger til registrering og tilbagevendende omkostninger vedrørende det løbende tilsyn). Dette er tilfældet for kreditvurderingsbureauer (jf. Kommissionens delegerede forordning (EU) nr. 272/2012) og transaktionsregistre (jf. Kommissionens delegerede forordning (EU) nr. 1003/2013).

I henhold til dette lovgivningsmæssige forslag vil ESA'erne få overdraget nye opgaver, som har til formål at fremme konvergens i forbindelse med tilgange til tilsyn med IKT-tredjepartsrisici i den finansielle sektor ved at lade kritiske tredjepartsudbydere af IKT-tjenester omfatte af en EU-tilsynsramme.

Den tilsynsramme, der påtænkes i dette forslag, bygger på den eksisterende institutionelle arkitektur på området for finansielle tjenesteydelser, hvorved Det Fælles Udvalg af ESA'er sikrer koordinering på tværs af sektorer af alle anliggender, der vedrører IKT-risici, i overensstemmelse med dets opgaver vedrørende cybersikkerhed og med støtte fra det relevante underudvalg (tilsynsforummet), som udfører det forberedende arbejde med henblik på individuelle afgørelser og kollektive henstillinger, der rettes til kritiske tredjepartsudbydere af IKT-tjenester.

Gennem denne ramme tillægges de ESA'er, der er udnævnt som ledende tilsynsførende for hver af disse kritiske tredjepartsudbydere af IKT-tjenester, beføjelser til at sikre, at udbydere af digitale tjenester, der opfylder en vigtig rolle for at sikre en velfungerende finansiel sektor, overvåges i tilstrækkelig grad på paneuropæisk plan. Tilsynsopgaverne er beskrevet i forslaget og præciseres yderligere i begrundelsen. De omfatter rettigheder til at anmode om alle relevante oplysninger og al relevant dokumentation med henblik på foretage generelle undersøgelser og inspektioner for at efterkomme henstillinger og efterfølgende forelægge rapporter om de iværksatte tiltag eller gennemførte afhjælpende foranstaltninger med henblik på at efterkomme de pågældende henstillinger.

For at varetage de nye opgaver, der påtænkes i dette forslag, ansætter ESA'erne yderligere personale, der er specialiseret i IKT-risici, og som fokuserer på at vurdere afhængighed af tredjeparter.

Behovene for menneskelige ressourcer kan anslås til 6 FTÆ for hver myndighed (5 AD og 1 AST til støtte for AD'erne). ESA'erne vil også pådrage sig yderligere IT-omkostninger, som anslås til 500 000 EUR (engangsomkostninger) samt 50 000 EUR om året for hver af de tre ESA'er til vedligeholdelsesomkostninger. Et vigtigt element i varetagelsen af de nye opgaver er de missioner, der foretager inspektioner på steder og revisioner, som kan anslås til 200 000 EUR pr. år for hver ESA. Udgifter til oversættelse af de forskellige dokumenter, som ESA'erne modtager fra de kritiske tredjepartsudbydere af IKT-tjenester, er ligeledes medregnet i linjen for driftsomkostninger og beløber sig til 350,000 EUR pr. år.

Alle ovennævnte administrative omkostninger finansieres fuldt ud af de årlige gebyrer, som ESA'erne opkræver hos de kritiske tredjepartsudbydere af IKT-tjenester, der er omfattet af tilsynet (ingen virkninger for EU-budgettet).